Acronis® Internet Security Suite 2010



Benutzerhandbuch

Acronis Internet Security Suite 2010
Benutzerhandbuch

Veröffentlicht 2010.02.02

Rechtlicher Hinweis

Inhaltsverzeichnis

Vorwort

Dieses Benutzerhandbuch ist für alle Benutzer vorgesehen, die sich für **Acronis Internet Security Suite 2010** als Sicherheitslösung entschieden haben. Die in diesem Dokument beschriebenen Informationen sind nicht nur für IT-Profis gedacht, sondern auch für all diejenigen die sich nur in Ihrer Freizeit mit dem Computer beschäftigen.

Dieses Buch beschreibt Acronis Internet Security Suite 2010 und wird Sie durch den Installationsprozess führen und Ihnen erklären, wie das Produkt konfiguriert werden kann. Sie werden herausfinden wie Sie Acronis Internet Security Suite 2010 nutzen können, wie ein Update durchgeführt wird, wie Sie es testen und Ihren Bedürfnissen anpassen können. So lernen Sie optimal mit diesem Produkt umzugehen und es effektiv einzusetzen.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

1. Verwendete Konventionen

1.1. Typografie

Um die Lesbarkeit zu verbessern, werden verschiedene Arten von Textstilen verwendet. Die jeweiligen Bedeutungen entnehmen Sie bitte der nachfolgenden Tabelle.

Erscheinungsbild	Beschreibung
`sample syntax`	Syntaxbeispiele werden in einer Schriftart mit `fester Laufweite` angegeben.
http://www.acronis.de/support/	Verweise (Links) auf externe Inhalte wie z.B. Web-Seiten oder FTP-Server.
„Vorwort“ (S. ix)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
`filename`	Dateien und Verzeichnisse werden in einer Schriftart mit `fester Laufweite` angegeben.
option	Optionen wie z.B. Schaltflächen oder Checkbox-Elemente werden in **fett gedruckt** angegeben.
`sample code listing`	Beispielquelltexte werden in einer Schriftart mit `fester Laufweite` angegeben.

1.2. Symbole

Bei diesen Symbolen handelt es sich um Hinweise innerhalb des Textflusses welche mit einer kleinen Grafik markiert sind. Hierbei handelt es sich um Informationen die Sie in jedem Fall beachten sollten.



Anmerkung

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.



Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.



Warnung

Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

2. Buchstruktur

Das Buch besteht aus mehreren Teilen unterteilt in Hauptthemen. Ausserdem ist ein Glossar enthalten welcher einige technische Begriffe erklärt.

Installation und Deinstallation. Schritt-für-Schritt Anleitungen für die Installation des Acronis Internet Security Suite 2010 auf einem PC. Von der Prüfung der Systemvoraussetzungen bis hin zur erfolgreichen Installation werden Sie durch den gesamten Vorgang geleitet. Zudem erfahren Sie, wie Sie Acronis Internet Security Suite 2010 bei Bedarf deinstallieren können.

Erste Schritte. Enthält alle Informationen die Sie für die ersten Schritte im Acronis Internet Security Suite 2010 benötigen. Sie erhalten einen Überblick über die Benutzeroberfläche, erfahren wie Sie auf Warnungen reagieren, wie Sie Basis-Einstellungen vornehmen können und wie Sie Ihr Produkt registrieren.

Standard-Ansicht. Gibt einen Überblick über die fortgeschrittene Ansicht der Acronis Internet Security Suite 2010 Benutzeroberfläche.

Profi Modus. Beschreibt detailliert die Profi-Ansicht der Acronis Internet Security Suite 2010 Benutzeroberfläche. Ihnen wird beigebracht wie Sie Acronis Internet Security Suite 2010 konfigurieren und Handhaben können um den bestmöglich Schutz vor allen Arten von Gefahren (Schädlingen, Spam, Hackern, unpassendem Inhalt und so weiter) zu erhalten.

Integration in Windows und Third-Party Software. Beschreibt die Acronis Internet Security Suite 2010 Optionen im Windows Kontextmenü und die Toolbars in unterstützten Drittanbieter-Produkten.

Wie man. Bietet Vorgehensweisen um die allgemeinsten Aufgaben in Acronis Internet Security Suite 2010 schnell durchzuführen.

Fehlediagnose und Problemlösung. Beschreibt wie Sie Hilfe bzw. Unterstützung zu dem Produkt erhalten und erhält zusätzlich eine Liste mit den am häufigsten gestellten Fragen (FAQ).

Glossar. Im Glossar werden technische Ausdrücke und seltene Bezeichnungen erklärt, die in diesem Dokument zu finden sind.

Installation und Deinstallation

1. Systemanforderungen

Sie können Acronis Internet Security Suite 2010 nur auf Computern mit den folgenden Betreibssystemen installieren:

- Windows XP (32/64 bit) mit Service Pack 2 oder höher
- Windows Vista (32/64 bit) oder Windows Vista mit Service Pack 1 oder höher.
- Windows 7 (32/64 bit)

Stellen Sie vor der Installation sicher, dass Ihr Computer die Mindestanforderungen für Hardware und Software erfüllt.



Anmerkung

Um Informationen über Ihr Betriebssytem und Ihre Hardware zu erhalten, klicken Sie mit der rechten Maustaste **Arbeitsplatz** auf dem Desktop und wählen Sie **Eigenschaften** aus dem Menu.

1.1. Mindest-Systemanforderungen

- 450 MB verfügbarer Festplattenspeicher
- 800 MHz Prozessor
- Arbeitsspeicher:
  - 512 MB für Windows XP
  - 1 GB für Windows Vista/Windows 7
- Internet Explorer 6.0
- .NET Framework 1.1 (befindet sich ebenfalls im Installationspaket)

1.2. Empfohlene Systemanforderungen

- 600 MB verfügbarer Festplattenspeicher
- Intel CORE 2 Duo (1.66 GHz) oder gleichwertiger Prozessor
- Arbeitsspeicher:
  - 1 GB für Windows Vista/Windows 7
  - 1.5 GB für Windows Vista
- Internet Explorer 7 (oder höher)
- .NET Framework 1.1 (befindet sich ebenfalls im Installationspaket)

1.3. Unterstützte Software

Der Antiphishingschutz arbeitet nur für:

- Internet Explorer 6.0 (oder höher)
- Mozilla Firefox 2.5 (oder höher)
- Yahoo Messenger 8.5 (oder höher)
- Windows Live Messenger 8 (oder höher)

Instant Messaging (IM) Verschlüsselung arbeitet nur für:

- Yahoo Messenger 8.5 (oder höher)
- Windows Live Messenger 8 (oder höher)

Der Antispam-Schutz steht für alle POP3/SMTP E-Mail-Clients zur Verfügung. Die Acronis Internet Security Suite 2010 Antispam Toolbar ist integriert in:

- Microsoft Outlook 2000 / 2003 / 2007
- Microsoft Outlook Express
- Microsoft Windows Mail
- Thunderbird 2.0.0.17

2. Installation wird vorbereitet

Bevor Sie Acronis Internet Security Suite 2010 installieren, sollten Sie für eine reibungslose Installation sicherstellen, daß Sie folgende Schritte durchgeführt haben:

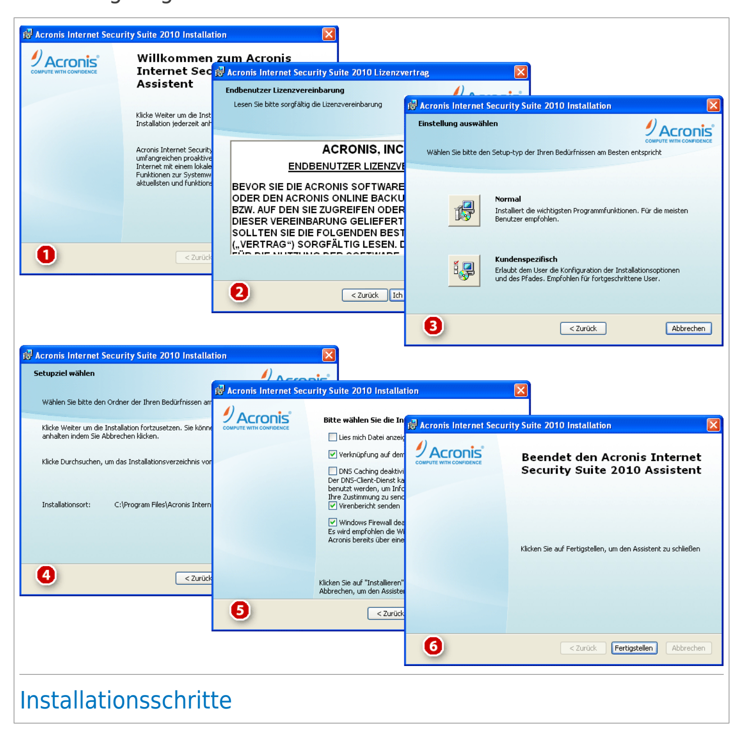
- Stellen Sie sicher, daß der Zielcomputer für die Acronis Internet Security Suite 2010 Installation die Systemvoraussetzungen erfüllt. Wenn Ihr Computer nicht die minimalen Systemvoraussetzungen erfüllt, wird sich Acronis Internet Security Suite 2010 nicht installieren lassen. Wird die System-Konfiguration nachträglich verändert so daß die Voraussetzungen nicht mehr erfüllt sind, kann es zu Leistungseinbußen und Stabilitätsproblemen kommen. Um die komplette Liste der Systemanforderungen zu überprüfen, lesen Sie bitte *„Systemanforderungen“* (S. 2).
- Melden Sie sich mit einem Administrator-Konto am Computer an.
- Entfernen Sie andere Sicherheits-Software von Ihrem Computer. Die gleichzeitige Nutzung von mehrerer Sicherheits-Programme kann die jeweilige Funktion stören und massive Probleme mit Ihrem Computer verursachen. Windows Defender wird standardmäßig deaktiviert bevor die Installation startet.
- Deaktivieren oder entfernen Sie jedwedes Firewall-Programm welches auf dem PC läuft. Die gleichzeitige Nutzung von mehrerer Sicherheits-Programme kann die jeweilige Funktion stören und massive Probleme mit Ihrem Computer verursachen. Windows Firewall wird standardmäßig deaktiviert bevor die Installation startet.

3. Acronis Internet Security Suite 2010 installieren

Sie können die Installationsdatei von der Acronis-Webseite erwerben und herunterladen: http://www.acronis.de/homecomputing/

Suchen Sie die Installationsdatei und klicken Sie doppelt auf diese, um Acronis Internet Security Suite 2010 zu installieren. Das startet einen Assistenten, der Sie durch den Installationsprozess führt.

Der Installer wird zuerst Ihr Sytem untersuchen, um die Installation zu bestätigen. Wenn die Installation bestätigt ist, erscheint der Installationsassistent. Die folgende Abbildung zeigt die Schritte des Installationsassistenten.



Installationsschritte

Folgen Sie diesen Schritten um Acronis Internet Security Suite 2010 zu installieren:

1. Klicken Sie auf **Weiter**. Sie können die Installation zu jeder Zeit abbrechen, indem Sie **Abbrechen** klicken.

   Acronis Internet Security Suite 2010 weist Sie daraufhin, ob weitere Antiviren-Programme auf Ihrem Computer installiert sind. Klicken Sie auf

Entfernen, um das betreffende Produkt zu deinstallieren. Sollten Sie fortfahren wollen ohne das entsprechende Produkt zu entfernen, dann klicken Sie auf **Weiter**.



Warnung

Es wird dringend empfohlen, andere Antiviren-Programme zuvor zu deinstallieren. Eine zeitgleiche Verwendung mehrerer Antiviren-Produkte kann Instabilität und Systemabstürze zur Folge haben.

2. Lesen Sie die Lizenzvereinbarung und klicken Sie auf **Ich stimme zu**.



Wichtig

Wenn Sie diesen Bedingungen nicht zustimmen, klicken Sie auf **Abbrechen**. Die Installation wird abgebrochen und Sie werden das Setup verlassen.

3. Wählen Sie die Installationsart, die durchgeführt werden soll.
   - **Standard** - um das Programm mit den Standard-Optionen sofort zu installieren. Wenn Sie diese Option wählen, gehen Sie zu schritt 6.
   - **Individuell** - um die Optionen zu konfigurieren und das Programm zu installieren. Mit dieser Option können Sie den Installationspfad ändern.
4. Standardmäßig wird Acronis Internet Security Suite 2010 im Ordner `C:\Program Files\Acronis Internet Security Suite\Acronis Internet Security Suite 2010` installiert. Wenn Sie den Installationpfad ändern möchten, klicken Sie auf **Durchsuchen** und wählen Sie den Ordner in dem Sie Acronis Internet Security Suite 2010 installieren möchten.

   Klicken Sie auf **Weiter**.
5. Optionen bezüglich der Installation auswählen. Die empfohlenen Optionen werden standardmässig ausgewählt:
   - **Öffnen der Readme Datei** - öffnen der Readme Datei am Ende der Installation.
   - **Verknüpfung auf dem Desktop erstellen** - um ein Symbol von Acronis Internet Security Suite 2010 am Ende der Installation auf Ihrem Desktop zu speichern.
   - **DNS Caching deaktivieren** - um DNS (Domain Name System) Caching zu deaktivieren. Der DNS-Client-Dienst kann von schädlichen Anwendungen benutzt werden, um Informationen über das Netzwerk ohne Ihre Zustimmung zu senden.
   - **Virus Berichte senden** - um Virus Berichte zur Analyse and das Acronis Labor zu senden. Bitte beachten Sie, dass diese Berichte weder vertrauliche Daten, wie Ihren Namen und Ihre IP Adresse, enthalten, noch werden diese Daten für kommerzielle Zwecke verwendet.
   - **Windows-Firewall ausschalten** -um die Windows eigene Firewall zu deaktivieren.



Wichtig

Wir empfehlen die Windows-basierte Firewall zu deaktivieren. Acronis Internet Security Suite 2010 beinhaltet eine erweiterte Firewall. Der Gebrauch von zwei Firewalls auf ein und demselben Computer kann zu Problemen führen.

- **Ausschalten von Windows-Defender** - um den Windows-Defender zu deaktivieren; diese Option erscheint nur bei Windows Vista.

Klicken Sie auf **Installieren**, um mit der Installation des Produkts zu beginnen. Acronis Internet Security Suite 2010 wird zuerst .NET Framework 1.1. installieren, falls dies noch nicht installiert ist.

6. Warten Sie, bis die Installation beendet ist und klicken Sie **Beenden**. Sie werden aufgefordert, Ihren Computer neu zu starten, damit der Setup-Assistent den Installationsprozess fertigstellen kann. Wir raten dazu, das so bald wie möglich zu tun.

4. Produkt-Aktivierung

Wenn Sie Ihren Computer nach der Installation neu starten, wird das Programm für 30 Tage in einem Testmodus laufen. Das Produkt muss während dieser Periode aktiviert werden. Falls Sie das Produkt während dieses Zeitfensters nicht aktivieren, wird es aufhören zu arbeiten.

Wenn Sie das Produkt erwerben, erhalten Sie eine 16-stellige Seriennummer per E-Mail. Die zur Produktaktivierung benötigte 64-stellige Seriennummer wird an Ihre E-Mail-Adresse geschickt, nachdem Sie Ihre 16-stellige Seriennummer auf der Registrierungswebseite eingegeben haben.

Beachten Sie, dass Ihre 1-jährige Produktlizenz beginnt, sobald Ihnen die 64-stellige Seriennummer zugeschickt wird. Nach Ablauf des Benutzungszeitraums verfällt Ihre Lizenz und können Sie das Produkt nicht mehr verwenden. Sie müssen eine neue Lizenz kaufen, um das Produkt wieder freizuschalten. Ihnen wird dann per E-Mail eine neue 16-stellige Seriennummer zugesendet, woraufhin Sie die Aktivierungsprozedur erneut durchführen müssen.

Die Aktivierung Schritt für Schritt

Wenn Sie das Programm zum ersten Mal starten, werden Sie nach der 64-stelligen Seriennummer gefragt.

Fall 1 – Wenn Sie die 64-stellige Seriennummer haben:

1. Klicken Sie auf die Schaltfläche **Ja, habe ich**.
2. Fügen Sie auf der nächsten Seite die Seriennummer in das entsprechende Feld ein (durch Verwendung der Tastenkombination Strg+V).
3. Klicken Sie auf die Schaltfläche **Aktivieren**.

Fall 2 – Wenn Sie keine 64-stellige, aber die 16-stellige Seriennummer haben:

1. Klicken Sie auf die Schaltfläche **Seriennummer erhalten**.
2. Geben Sie auf der Webseite Ihre Acronis Anmeldedaten, die 16-stellige Seriennummer und Ihre E-Mail-Adresse ein. Sie erhalten die 64-stellige Seriennummer als Nachricht an die von Ihnen angegebene E-Mail-Adresse zugeschickt.

   Sollten Sie bisher noch über kein Acronis-Konto verfügen, so wird dieses unter Verwendung der von Ihnen bei Registrierung angegebenen persönlichen Informationen erstellt.
3. Öffnen Sie die empfangenen E-Mail-Nachricht und kopieren Sie die Seriennummer.
4. Wechseln Sie zum Programm und klicken Sie auf die Schaltfläche **Ja, habe ich**.

5. Fügen Sie auf der nächsten Seite die Seriennummer in das entsprechende Feld ein (durch Verwendung der Tastenkombination Strg+V).
6. Klicken Sie auf die Schaltfläche **Aktivieren**.

Fall 3 – Wenn Sie weder eine 16- noch 64-stellige Seriennummer haben:

1. Klicken Sie auf den Link **Online kaufen**.
2. Erwerben Sie das Produkt. Die 16-stellige Seriennummer wird Ihnen per E-Mail zugeschickt.
3. Führen Sie alle Schritte von 'Fall 2' aus.

Fall 4 – Wenn Sie keine Seriennummer haben und das Produkt zuerst testen wollen:

1. Klicken Sie auf die Schaltfläche **Später**. Das Produkt ist während des Testzeitraums voll funktionsfähig.
2. Falls Sie sich zum Kauf des Produkts entschließen, führen Sie alle Schritte von 'Fall 3' aus.

5. Acronis Internet Security Suite 2010 reparieren oder entfernen

Wenn Sie Acronis Internet Security Suite 2010 reparieren oder entfernen wollen, folgen Sie dem Pfad vom Windows Start Menu: **Start** → **Programme** → **Acronis Internet Security Suite 2010** → **Reparieren oder Entfernen**.

Sie werden aufgefordert, Ihre Auswahl zu bestätigen. Klicken Sie dazu auf **Weiter**. Ein neues Fenster mit folgenden Auswahloptionen wird angezeigt:

- **Reparieren** - dient zur Neuinstallation sämtlicher Programmkomponenten, die beim vorhergegangenen Setup installiert wurden.

  Wenn Sie Reparieren von Acronis Internet Security Suite 2010 wählen erscheint ein neues Fenster. Klicken Sie auf **Reparieren** um die Reparatur zu starten.

  Starten Sie den Computer neu wenn Sie dazu aufgefordert werden, anschliessend klicken Sie auf **Installieren** um Acronis Internet Security Suite 2010 neu zu installieren.

  Wenn der Installationsprozess abgeschlossen wurde erscheint ein neues Fenster. Klicken Sie auf **Fertigstellen**.

- **Entfernen** - dient zum Entfernen aller installierten Komponenten.



Anmerkung

Wir empfehlen die Option **Entfernen** zu verwenden um eine saubere Neuinstallation durchzuführen.

Wenn Sie Acronis Internet Security Suite 2010 entfernen wählen erscheint ein neues Fenster.



Wichtig

Durch das Entfernen von Acronis Internet Security Suite 2010 sind Sie nicht länger vor Viren, Spyware und Hackern geschützt. Wenn Sie möchten das die Windows Firewall und Windows Defender (Nur in Windows Vista) nach der Deinstallation wieder aktiviert werden, selektieren Sie die entsprechende Option.

Klicken Sie auf **Entfernen** um mit der Deinstallation von Acronis Internet Security Suite 2010 zu beginnen.

Sobald der Entfernungsprozess abgeschlossen wurde erscheint ein neues Fenster. Klicken Sie auf **Fertigstellen**.



Anmerkung

Nachdem die Deinstallation beendet wurde empfehlen wir Ihnen den Ordner `Acronis Internet Security Suite` im Ordner `Programme` zu löschen.

Erste Schritte

6. Übersicht

Sobald Sie Acronis Internet Security Suite 2010 installiert haben ist Ihr Computer geschützt.

6.1. Acronis Internet Security Suite 2010 öffnen

Sie erreichen die Benutzeroberfläche von Acronis Internet Security Suite 2010 über das Windows-Startmenü: **Start → Programme → Acronis Internet Security Suite 2010 → Acronis Internet Security Suite 2010** oder, schneller per Doppelklick auf das Acronis Symbol in der Systemleiste.

6.2. Benutzeroberfläche Ansichtsmodus

Acronis Internet Security Suite 2010 entspricht den Bedürfnissen sowohl von Profis als auch von Beginnern. Die grafische Benutzeroberfläche ist so konzipiert, dass Sie für jeden Benutzer anpassbar ist.

Sie können die Benutzeroberfläche in einem von 3 Modi anschauen, abhängig von Ihrer Computer-Erfahrung und Ihrer Erfahrung mit Acronis.

Modus	Beschreibung
Basis-Ansicht	Geeignet für Anfänger und für diejenigen, die Acronis Internet Security Suite 2010 ohne Aufwand zum Schutz ihres Computers und ihrer Daten nutzen wollen. Diese Ansicht ist einfach in der Handhabung und verlangt minimalen Aufwand Ihrerseits. Sie müssen nur die existierenden Punkte beheben, wenn Acronis Internet Security Suite 2010 Sie dazu auffordert. Ein intuitiver Schritt für Schritt Assistent hilft Ihnen dabei. Zusätzlich können Sie gewöhnliche Aufgaben ausführen, wie das Aktualisieren der Acronis Internet Security Suite 2010 Virensignaturen und Produktdateien oder die Prüfung Ihres Computers.
Standard-Ansicht	Für Benutzer mit durchschnittlicher Computer-Erfahrung, erweitert diese Ansicht die Basis-Einstellungen. Sie können offene Punkte separat beheben und wählen welche Punkte überwacht werden. Ferner können Sie die Acronis Produkte auf entfernten Computern in Ihrem Haushalt verwalten.

Modus	Beschreibung
Profi-Modus	Für technisch fortgeschrittene Anwender, erlaubt Ihnen diese Ansicht jede Funktion von Acronis Internet Security Suite 2010 zu konfigurieren. Sie können auch alle Funktionen benutzen, um Ihren Computer und Ihre Daten zu schützen.

Die Benutzeroberfläche wird in der Grundeinstellung im 'Intermediate-Modus' dargestellt. Um den Modus der Benutzeroberfläche zu wechseln, folgen Sie diesen Schritten:

1. Öffnen Sie Acronis Internet Security Suite 2010.
2. Klicken Sie oben rechts im Fenster den **Einstellungen** Schalter.
3. In den Einstellungen für die Benutzeroberfläche, klicken Sie den Pfeil und wählen sie den Modus vom menü.
4. Klicken Sie **OK**, um die Änderungen zu speichern und zu übernehmen.

6.2.1. Basis-Ansicht

Wenn Sie ein Computer-Anfänger sind, ist die Basis-Ansicht der Benutzeroberfläche wahrscheinlich die beste Wahl für Sie. Dieser Modus ist einfach zu handhaben und erfordert nur minimale Interaktion Ihrereseits.



Basis-Ansicht

Das Fenster ist in 4 Abschnitte unterteilt:

- **Sicherheitsstatus** informiert Sie über die Risiken die die Sicherheit Ihres Systems gefährden, und hilft diese zu beheben. Durch Klicken auf **Alles Risisken beheben** erscheint ein Assistent der Ihnen helfen wird Bedrohungen für PC und Daten zu entfernen. Weitere Informationen finden Sie unter dem Kapitel *„Alle beheben“* (S. 33).
- **Schützen Sie Ihren PC** lässt Sie alle Aufgaben zum Schutz von Computer und Daten finden. Die verfügbaren Aufgaben die Sie durchführen können sind unterschiedlich, abhängig von dem vorgewählten Nutzungsprofil.
  - Die **Jetzt Prüfen** Schaltfläche startet eine standard Prüfung ihres Systems nach Viren, Spyware und anderer Malware. Der Antivirusprüfassistend wird erscheinen und Sie durch den Prüfprozess führen. Weitere Informationen zu diesem Assistenten finden Sie unter *„Antivirus Prüfassistent“* (S. 44).
  - Die option **Jetzt aktualisieren** hilft Ihnen die Virensignaturen und Produktdateien von Acronis Internet Security Suite 2010 zu aktualisieren. Ein neues Fenster wird erscheinen, in dem Sie Status des Updates sehen können. Wenn neue Updates erkannt werden, werden sie automatisch auf Ihren PC heruntergeladen und installiert.
  - Wenn das **Standard** Profil ausgewählt ist, wird die **Schwachstellenprüfung** Schaltfläche einen Assistenten starten der Ihnen dabei hilft Systemschwachstellen zu finden und zu beheben, wie z.B. veraltete Software oder fehlende Windows Updates. Weitere Informationen finden Sie unter *„Schwachstellenprüfassistent“* (S. 56).
  - Wenn das **Kindersicherungs**-Profil ausgewählt ist, lässt Sie die **Kindersicherungs**-Schaltfläche die Einstellungen konfigurieren. Kindersicherung begrenzt die Rechner- und Online-Aktivitäten Ihrer Kinder, basierend auf die von Ihnen festgelegeten Regeln. Beschränkungen können das Blockieren von unsachgemässen Web-Seiten beinhalten, sowie begrenzten Spiele- und Internet-Zugriff gemäss des festgelegten Zeitplans. Für weitere Informationen zum konfigurieren der Kindersicherung lesen Sie bitte *„Kindersicherung“* (S. 173).
  - Wenn der **Spiele** Modus ausgewählt ist, erlaubt die **Spiele Modus Ein/Aus schalten** Schaltfläche das Aktivieren/Deaktivieren des Spiele Modus. Der Spiele-Modus ändert die Schutzeinstellungen zeitweise, dass ihr Einfluss auf die Leistungsfähigkeit des Systems so gering wie möglich ist.
- **Schützen Sie Ihren PC** lässt Sie alle Aufgaben zum Schutz von Computer und Daten finden.
  - **Datei zum Tresor hinzufügen** - Startet den Assistenten zum Speichern Ihrer wichtigen Dateien/Dokumente in verschlüsselten Datentresoren.
  - **Tiefgehende Systemprüfung** startet einen kompletten Scan Ihres Systems auf alle Arten der Malware.

- **Meine Documente Prüfung** prüft die am häufigsten benutzten Ordner auf Viren und andere Malware: `Meine Documente` und `Desktop`. Dies gewährleistet die Sicherheit Ihrer Dokumente, einen sicheren Arbeitsplatz und das saubere Laufen von Anwendungen beim Systemstart.

- **Nutzungsprofil** zeigt das aktuell gewählte Nutzungsprofil an. Das Nutzungsprofil reflektiert die hauptsächlich durchgeführten Aktivitäten auf dem Computer. Abhängig von Nutzungsprofil, wird die Benutzeroberfläche sortiert, damit Sie bequem auf Ihre bevorzugten Aufgaben zugreifen können.

  Wenn Sie in ein anderes Profil wechseln möchten oder das momentane Profil bearbeiten wollen, klicken Sie das auf das Profil und folgen dem Link Konifgurationsassistent.

Sie können in der oberen, rechten Ecke des Fensters die Schaltfläche **Einstellungen** sehen. Sie öffnet ein Fenster, wo Sie den Modus der Benutzeroberfläche ändern können und die Haupteinstellungen der Acronis Internete Security Suite 2010 aktivieren oder deaktivieren können. Für weitere Informationen lesen Sie bitte *„Konfigurieren der Grundeinstellungen“* (S. 36).

In der rechten unteren Ecke des Fensters findes Sie einige nützliche Links.

Link	Beschreibung
Kaufen/Verlängern	Öffnet eine Webseite von welcher Sie den Lizenzschlüssel für Ihre Acronis Internet Security Suite 2010 erwerben können.
Lizenz	Bietet Ihnen die Möglichkeit einen Seriennummer einzugeben und den Registrierungsstatus zu betrachten.
Support	Bietet Ihnen die Möglichkeit das Acronis Support Team zu kontaktieren.
Hilfe anzeigen	Gibt Ihnen Zugriff auf eine Hilfedatei, die Sie bei der Verwendung von Acronis Internet Security Suite 2010 unterstützt.
Protokolle	Zeigt Ihnen eine detaillierte Historie aller von Acronis Internet Security Suite 2010 auf Ihrem System durchgeführten Aufgaben.

6.2.2. Standard-Ansicht

Die Standard-Ansicht ist ausgelegt für Benutzer mit durchschnittlich guten PC-Kenntnissen, die Oberfläche gibt Ihnen Zugriff auf alle grundlegenden Module. Sie sollten Warnungen und kritische Alarme verfolgen und unerwünschte Risiken beheben.



Standard-Ansicht

Die Standard-Ansicht besteht aus fünf Tabs. Die folgende Tabelle beschreibt in Kürze jedes Tab. Für weitere Informationen lesen Sie bitte „Standard-Ansicht“ (S. 82) diesen Teil des Benutzerhandbuchs.

Tab	Beschreibung
Dashboard	Zeigt den Sicherheitsstatus Ihres Systems an und bietet Ihnen die Möglichkeit das Benutzerprofil zurückzusetzen.
Sicherheit	Zeigt den Status der Sicherheitsmodule an (Antivirus, Antiphishing, Firewall, Antispam, IM-Verschlüsselung, Privatsphäre, Prüfung auf Anfälligkeit und Update-Module) sowie Links zu Antivirus-, Update- und Anfälligkeitsprüfungs-Aufgaben.
Kindersicherung	Zeigt den Status des Kindersicherungsmoduls an. Die Kindersicherung erlaubt es Ihnen den Zugriff Ihrer Kinder auf das Internet und für bestimmte Anwendungen einzuschränken.
Datentresor	Zeigt den Status des Dateischutzes an sowie Links zum Dateischutz.
Netzwerk	Zeigt die Struktur des Acronis Home-Netzwerkes an. Dies ist wo Sie verschiedene Aktionen durchführen, um Acronis Produkte die in Ihrem Heimnetzwerk installiert sind, konfigurieren und verwalten zu können. Auf diesem Wege

Tab	Beschreibung
	können Sie die Sicherheit Ihres Heimnetzwerks von einem einzelnen Computer aus verwalten.

Sie können in der oberen, rechten Ecke des Fensters die Schaltfläche **Einstellungen** sehen. Sie öffnet ein Fenster, wo Sie den Modus der Benutzeroberfläche ändern können und die Haupteinstellungen der Acronis Internete Security Suite 2010 aktivieren oder deaktivieren können. Für weitere Informationen lesen Sie bitte *„Konfigurieren der Grundeinstellungen“* (S. 36).

In der rechten unteren Ecke des Fensters findes Sie einige nützliche Links.

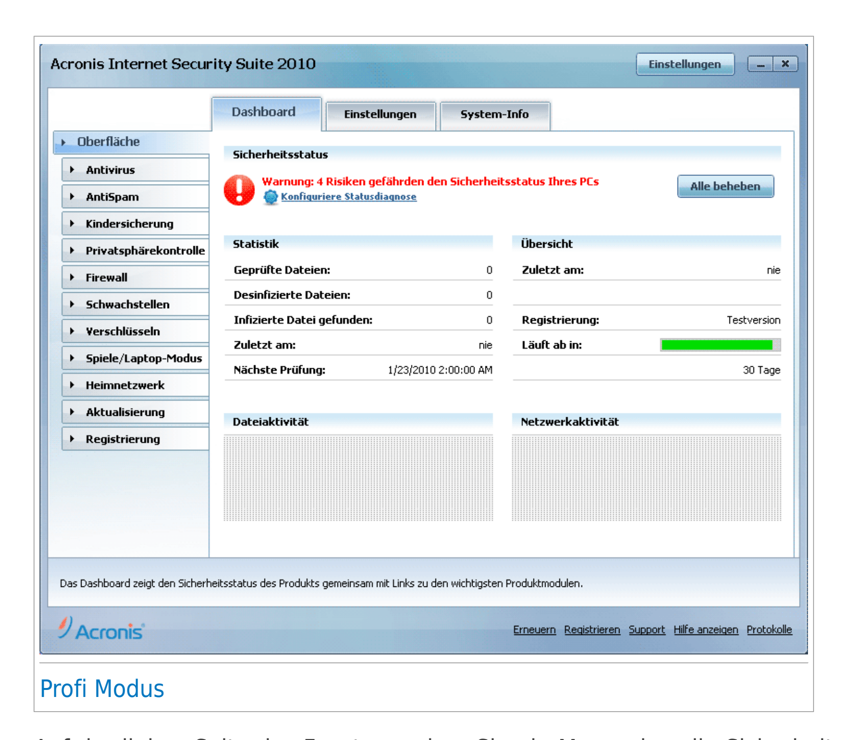
Link	Beschreibung
Kaufen/Verlängern	Öffnet eine Webseite von welcher Sie den Lizenzschlüssel für Ihre Acronis Internet Security Suite 2010 erwerben können.
Lizenz	Bietet Ihnen die Möglichkeit einen Seriennummer einzugeben und den Registrierungsstatus zu betrachten.
Support	Bietet Ihnen die Möglichkeit das Acronis Support Team zu kontaktieren.
Hilfe anzeigen	Gibt Ihnen Zugriff auf eine Hilfedatei, die Sie bei der Verwendung von Acronis Internet Security Suite 2010 unterstützt.
Protokolle	Zeigt Ihnen eine detaillierte Historie aller von Acronis Internet Security Suite 2010 auf Ihrem System durchgeführten Aufgaben.

6.2.3. Profi Modus

Die Profi-Ansicht gibt Ihnen Zugriff auf jede einzelne Komponente von Acronis Internet Security Suite 2010. Hier können Sie Acronis Internet Security Suite 2010 im Einzelnen konfigurieren.



Anmerkung
Fortgeschrittenen Ansicht ist geeignet für Anwender die über mehr als durchschnittliche PC-Kenntnisse verfügen, jemand dem die Art von existrierenden PC-Bedrohungen und wie ein Sicherheitsprogramm arbeitet bewusst ist.



Profi Modus

Auf der linken Seite des Fensters sehen Sie ein Menu, das alle Sicherheitsmodule beinhaltet: Jedes Modul verfügt über ein oder mehrere Tabs in welchem Sie die dazugehörigen Sicherheitseinstellungen konfigurieren oder Sicherheits- und administrative Aufgaben durchführen können. Die folgende Auflistung beschreibt in Kürze jedes Modul. Weitere Informationen finden Sie unter dem Kapitel „Profi Modus“ (S. 103) in diesem Handbuch.

Modul	Beschreibung
Allgemein	Hier haben Sie Zugriff zu den allgemeinen Einstellungen. Sie können hier auch das Dashboard und detaillierte Systeminformationen betrachten.
Antivirus	Bietet Ihnen die Möglichkeit Ihr Virus-Schild und Prüfprozesse zu konfigurieren, Ausnahmen festzulegen und das Quarantäne-Modul zu konfigurieren.
Antispam	Bietet Ihnen die Möglichkeit Ihr Postfach SPAM-frei zu halten und die Antispam-Einstellungen detailliert zu konfigurieren.

Modul	Beschreibung
Kindersicherung	Bietet Ihnen die Möglichkeit Ihre Kinder gegen jugendgefährdende Inhalte zu schützen. Nutzen Sie dabei Ihre selbst festgelegten Regeln.
Privatsphäre-Kontrolle	Bietet Ihnen die Möglichkeit Datendiebstahl von Ihrem Computer vorzubeugen und Ihre Privatsphäre zu schützen während Sie online sind.
Firewall	Erlaubt es Ihnen Ihren Computer für unerlaubte Zugriffe von Aussen und Innen zu schützen. Ziemlich ähnlich dem Sicherheitsbeamten an einer Tür - wird es ein wachsames Auge auf Ihre Internetverbindung haben und beobachten wem der Zugriff zum Internet zu erlauben und wer zu blockieren ist.
Schwachstellen	Bietet Ihnen die Möglichkeit wichtige Software auf Ihrem PC stets auf dem neusten Stand zu halten.
Verschlüsselung	Bietet Ihnen die Möglichkeit Unterhaltungen über Yahoo und Windows Live (MSN) Messenger zu verschlüsseln und Ihre wichtigen Dateien, Ordner und Partitionen lokal zu verschlüsseln.
Spiele-/Laptop-Modus	Bietet Ihnen die Möglichkeit voreingestellte Prüfaufgaben, während Ihr Laptop über einen Akku betrieben wird. Weiterhin können Pop-ups und Benachrichtigungen vermieden werden während Sie spielen.
Netzwerk	Bietet Ihnen die Möglichkeit mehrere Computer in Ihrem Haushalt zu verwalten und konfigurieren.
Update	Bietet Ihnen die Möglichkeit die neusten Updates zu erhalten, das Produkt zu aktualisieren und den Update-Prozess genau zu konfigurieren.

Sie können in der oberen, rechten Ecke des Fensters die Schaltfläche **Einstellungen** sehen. Sie öffnet ein Fenster, wo Sie den Modus der Benutzeroberfläche ändern können und die Haupteinstellungen der Acronis Internete Security Suite 2010 aktivieren oder deaktivieren können. Für weitere Informationen lesen Sie bitte *„Konfigurieren der Grundeinstellungen“* (S. 36).

In der rechten unteren Ecke des Fensters findes Sie einige nützliche Links.

Link	Beschreibung
Kaufen/Verlängern	Öffnet eine Webseite von welcher Sie den Lizenzschlüssel für Ihre Acronis Internet Security Suite 2010 erwerben können.

Link	Beschreibung
Lizenz	Bietet Ihnen die Möglichkeit einen Seriennummer einzugeben und den Registrierungsstatus zu betrachten.
Support	Bietet Ihnen die Möglichkeit das Acronis Support Team zu kontaktieren.
Hilfe anzeigen	Gibt Ihnen Zugriff auf eine Hilfedatei, die Sie bei der Verwendung von Acronis Internet Security Suite 2010 unterstützt.
Protokolle	Zeigt Ihnen eine detaillierte Historie aller von Acronis Internet Security Suite 2010 auf Ihrem System durchgeführten Aufgaben.

6.3. Acronis Internet Security Suite 2010 einrichten

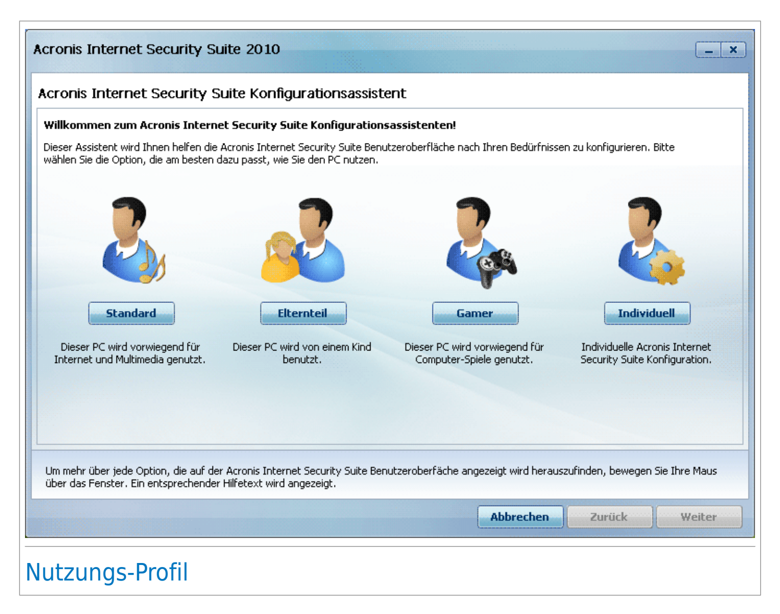
Acronis Security Suite 2010 ermöglicht Ihnen eine einfache Konfiguration seiner wichtigsten Einstellungen und der Benutzeroberfläche, indem Sie ein Benutzerprofil erstellen können. Das Nutzungsprofil reflektiert die hauptsächlich durchgeführten Aktivitäten auf dem Computer. Abhängig von Nutzungsprofil, wird die Benutzeroberfläche sortiert, damit Sie bequem auf Ihre bevorzugten Aufgaben zugreifen können.

Standardmäßig wird das Profil **Typisch** direkt nach der Installation von Acronis Internet Security Suite 2010 angewendet. Diese Profil ist passend für Computer, die hauptsächlich für Internet und Multimedia-Aktivitäten verwendet werden.

Folgen Sie diesen Schritten, um das Benutzerprofil zu rekonfigurieren:

1. Öffnen Sie Acronis Internet Security Suite 2010.
2. Klicken Sie oben rechts im Fenster den **Einstellungen** Schalter.
3. Klicken Sie in der Kategorie für die Einstellungen der Benutzeroberfläche auf **Profil rekonfigurieren**.
4. Folgen Sie dem Konfigurationsassistenten.

6.3.1. Schritt 1 - Profil auswählen



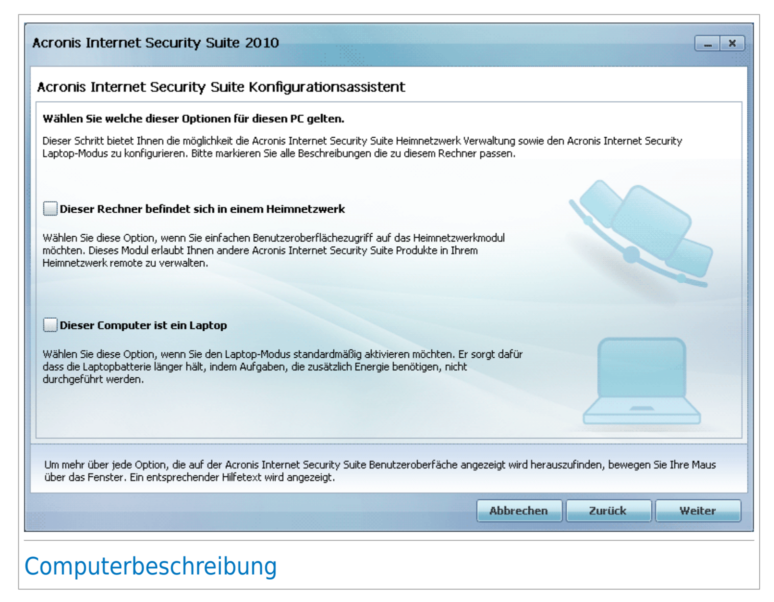
Nutzungs-Profil

Klicken Sie die Schaltfläche, die am besten die Nutzung dieses Computers beschreibt (das Nutzungsprofil).

Optionen	Beschreibung
Standard	Dieser PC wird vorwiegend für Internet und Multimedia genutzt.
Eltern	Klicken Sie hier, wenn dieser PC auch von Kindern benutzt wird und Sie deren Zugriff auf das Internet mit Hilfe der Kindersicherung einschränken möchten.
Spieler	Dieser PC wird vorwiegend für Computer-Spiele genutzt.
Benutzerdefiniert	Klicken Sie hier, wenn Sie alle Haupteinstellungen von Acronis Internet Security Suite 2010 konfigurieren möchten.

Sie können später das Nutzungsprofil von der Bedienoberfläche zurücksetzen.

6.3.2. Schritt 2 - Computerbeschreibung



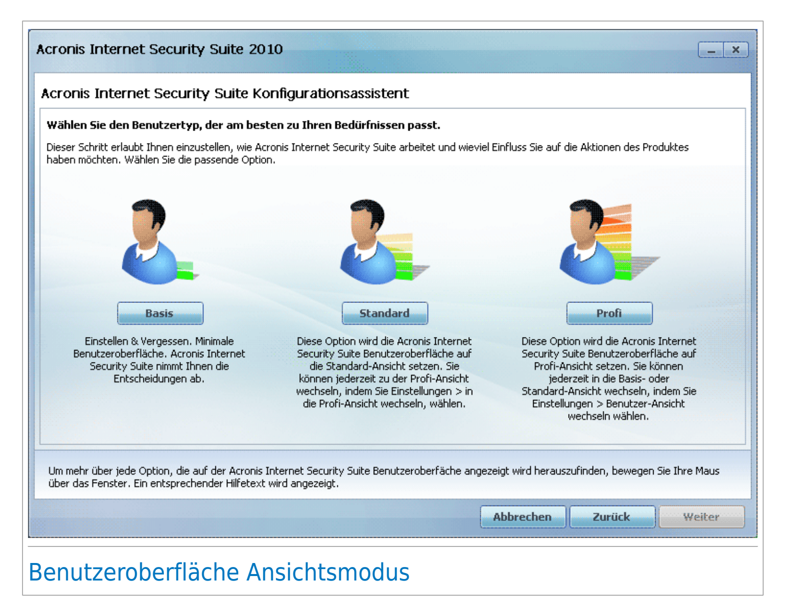
Computerbeschreibung

Wählen Sie die Optionen, die auf Ihren Computer zutreffen:

- **Dieser Rechner befindet sich in einem Heimnetzwerk.** Wählen Sie diese Option, wenn Sie das Acronis Produkt, welches auf diesem Computer installiert ist, per Remote verwalten möchten. Ein zusätzlicher Assistent hilft Ihnen, das Heim-Netzwerk Modul zu verwalten .
- **Dieser Computer ist ein Laptop.** Wählen Sie diese Option, wenn Sie den Laptop-Modus als Standard aktiviert haben möchten. Im Laptop-Modus werden keine geplanten Prüfungen durchgeführt, da diese mehr Systemresourcen benötigen und dies den Stromverbrauch erhöht.

Klicken Sie auf **Weiter**.

6.3.3. Schritt 3 - Bedienoberfläche auswählen



Benutzeroberfläche Ansichtsmodus

Klicken Sie die Schaltfläche, die am besten Ihre Computer Kentnisse beschreibt, um die passende Benutzerobflächen-Modus einzustellen. Sie können die Benutzeroberfläche in einem von 3 Modi anschauen, abhängig von Ihrer Computer-Erfahrung und Ihrer Erfahrung mit Acronis Internet Security Suite 2010.

Modus	Beschreibung
Basis-Ansicht	Geeignet für Anfänger und für diejenigen, die Acronis Internet Security Suite 2010 ohne Aufwand zum Schutz ihres Computers und ihrer Daten nutzen wollen. Diese Ansicht ist einfach in der Handhabung und verlangt minimalen Aufwand Ihrerseits. Sie müssen nur die existierenden Punkte beheben, wenn Acronis Internet Security Suite 2010 Sie dazu auffordert. Ein intuitiver Schritt für Schritt Assistent hilft Ihnen dabei. Zusätzlich können Sie gewöhnliche Aufgaben ausführen, wie das Aktualisieren der Acronis Internet Security Suite 2010 Virensignaturen und Produktdateien oder die Prüfung Ihres Computers.
Standard-Ansicht	Für Benutzer mit durchschnittlicher Computer-Erfahrung, erweitert diese Ansicht die Basis-Einstellungen.

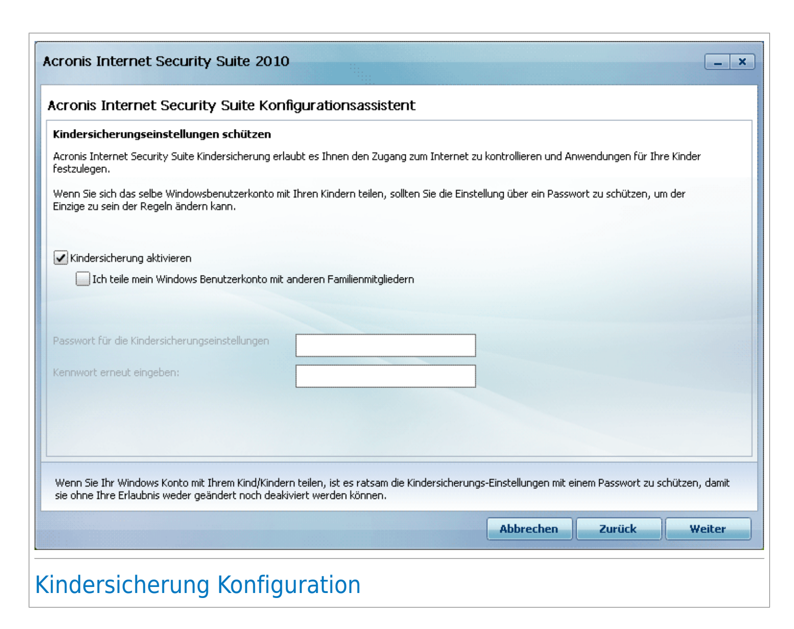
Modus	Beschreibung
	Sie können offene Punkte separat beheben und wählen welche Punkte überwacht werden. Ferner können Sie die Acronis Produkte auf entfernten Computern in Ihrem Haushalt verwalten.
Profi-Modus	Für technisch fortgeschrittene Anwender, erlaubt Ihnen diese Ansicht jede Funktion von Acronis Internet Security Suite 2010 zu konfigurieren. Sie können auch alle Funktionen benutzen, um Ihren Computer und Ihre Daten zu schützen.

6.3.4. Schritt 4 – Kindersicherung konfigurieren



Anmerkung

Dieser Schritt erscheint nur wenn Sie die **Benutzerdefiniert** Option bei Schritt 1 gewählt haben.



Kindersicherung Konfiguration

Die Kindersicherung gibt Ihnen die Möglichkeit den Zugriff auf das Internet und auf bestimmte Programme für jeden Benutzer mit einem Benutzerkonto auf dem System zu kontrollieren.

Um die Kindersicherung zu verwenden, führen Sie die folgenden Schritte durch:

1. Wählen Sie **Kindersicherung aktivieren**.

2. Wenn Sie Ihr Window-Benutzerkonto mit Kindern teilen, wählen Sie die entsprechende Option aus und geben ein Passwort zum Schutz der Kindersicherungseinstellungen in das dazugehörige Feld ein. Jeder der versucht das Passwort der Kindersicherungseinstellungen zu ändern muss zunächst das von Ihnen festgelegte Passwort angeben.

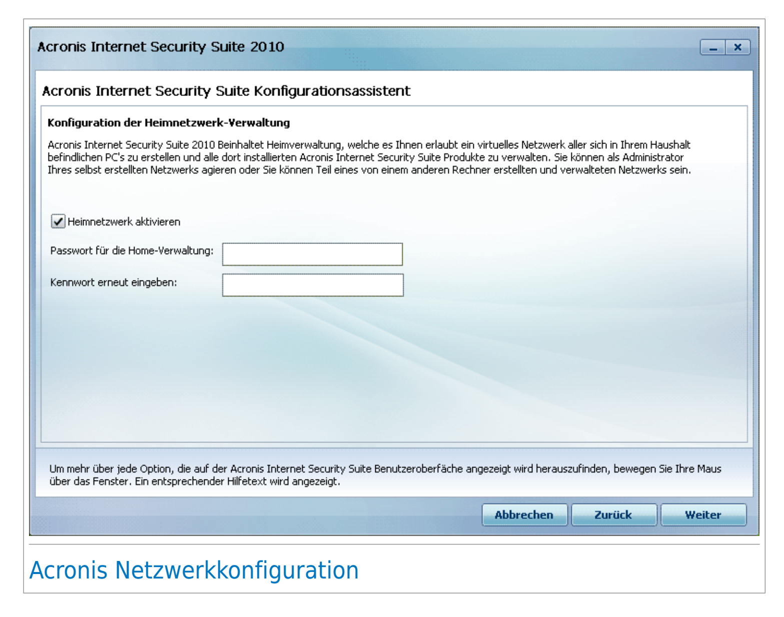
Klicken Sie auf **Weiter**.

6.3.5. Schritt 5 - Acronis Netzwerk konfigurieren



Anmerkung

Dieser Schritt erscheint nur wenn Sie bei Schritt 2, ausgewählt haben, dass der Computer mit einen Heim-Netzwerk verbunden ist.



Acronis Netzwerkkonfiguration

Mit Acronis Internet Security Suite 2010 können Sie ein virtuelles Netzwerk aller Computer in Ihrem Haushalt erstellen und kompatible, in diesem Netzwerk installierte Acronis-Produkte verwalten.

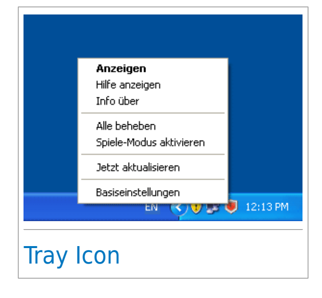
Wenn Sie möchten, dass dieser Computer Teil des Acronis Home-Netzwerkes sein soll, befolgen Sie folgende Schritte:

1. Wählen Sie **Heim-Netzwerk aktivieren**.
2. Geben Sie das selbe administrative Passwort in alle Editierfelder ein. Das Passwort gibt dem Administrator die Möglichkeit das Acronis Produkt, das auf diesem Computer installiert ist von einem anderen Computer aus zu verwalten.

Klicken Sie auf **Fertigstellen**.

6.4. System Tray Icon

Um das gesamte Produkt schneller zu verwalten, können Sie das Acronis Icon im System-Tray verwenden. Wenn Sie dieses Icon doppelklicken wird sich Acronis Internet Security Suite 2010 öffnen. Zudem öffnen Sie durch einen Rechtsklick ein Untermenu welches Ihnen einen schnelles verwalten des Acronis Internet Security Suite 2010 Produkts ermöglicht.



Tray Icon

- **Anzeigen** - öffnet die Hauptbedienoberfläche des Acronis Internet Security Suite 2010.
- **Hilfe** - öffnet die Hilfe-Datei, welche erklärt, wie man Acronis Internet Security Suite 2010 konfiguriert und benutzt.
- **Über** - Öffnet ein Fenster in welchem Sie Informationen über Acronis Internet Security Suite 2010 erhalten und Hilfe finden falls etwas unvorhergesehenes geschied.
- **Alle Risiken beheben** - hilft bestehende Sicherheitsschwachstellen zu entfernen. Falls die Option nicht verfügbar ist, so gibt es keine zu behebenden Probleme. Weitere Informationen finden Sie unter dem Kapitel *„Alle beheben“* (S. 33).
- **Spielemodus An / Aus** - aktiviert / deaktiviert Spielemodus.
- **Jetzt Aktualisieren** - startet ein sofortiges Update. Ein neues Fenster wird erscheinen, in dem Sie Status des Updates sehen können.
- **Grundeinstellungen** - öffnet ein Fenster in welchem man die Benutzeransicht ändern und Produkteinstellungen aktivieren oder deaktivieren kann. Für weitere Informationen lesen Sie bitte *„Konfigurieren der Grundeinstellungen“* (S. 36).

Das Acronis Symbol in der System Tray informiert Sie durch ein spezielles Symbol, wenn Probleme Ihren Computer betreffen, wie folgt:

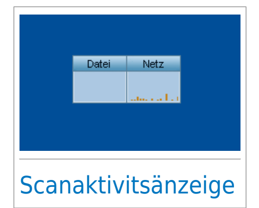
Rotes Dreieck mit einem Ausrufezeichen: Kritische Probleme betreffen die Sicherheit Ihres Systems. Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden.
Buchstabe G: Das Produkt arbeitet im Spiele Modus.

Wenn Acronis Internet Security Suite 2010 nicht funktioniert, ist das Symbol grau . Dies passiert normalerweise, wenn die Lizenz abgelaufen ist. Es kann auch vorkommen, wenn die Acronis Internet Security Suite 2010 Services nicht reagieren oder andere Fehler die normale Funktionsweise von Acronis Internet Security Suite 2010 einschränken.

6.5. Scanaktivitsänzeige

Die **Scan Aktions-Anzeige** ist eine graphische Visualisierung der Prüfaktivität auf Ihrem System. Dieses kleine Fenster ist standardmässig nur verfügbar in der Profi-Ansicht.

Die grauen Balken (die **Datei-Zone**) zeigen die Anzahl der gescannten Dateien pro Sekunde, auf einer Skala von 0 bis 50. Die orangen Balken in der **Netz-Zone** zeigen die Anzahl der transferierten KBytes (gesendet und empfangen aus dem Internet) pro Sekunde auf einer Skala von 0 bis 100.



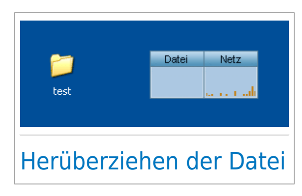
Scanaktivitsänzeige



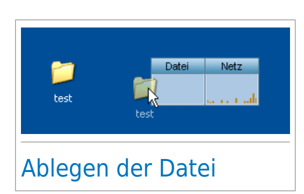
Anmerkung
Die Aktivitätsanzeige informiert Sie mit einem roten „X“, wenn der Echtzeitschutz oder die Firewall deaktiviert ist (**Datei** oder **Netz**).

6.5.1. Prüfe Dateien und Ordner

Sie können die Aktivitätsanzeige verwenden um kurzerhand Dateien und Ordner zu prüfen. Ziehen Sie die gewünschte Datei auf den **Datei-/Netzprüfmonitor**, wie auf den folgenden Bildern dargestellt.



Herüberziehen der Datei



Ablegen der Datei

Der Antivirusprüfassistend wird erscheinen und Sie durch den Prüfprozess führen. Weitere Informationen zu diesem Assistenten finden Sie unter *„Antivirus Prüfassistent“* (S. 44).

Scanoptionen. Die Prüfoptionen sind für bestmögliche Enteckungsraten vorkonfiguriert. Falls infizierte Dateien entdeckt werden wird Acronis Internet Security Suite 2010 versuchen diese zu desinfizieren (den Mailwarecode entfernen). Wenn die Desinfizierung fehlschlagen sollte wird Ihnen der Antivirus Prüfassistent andere Möglichkeiten anbieten wie mit den infizierten Dateien verfahren werden kann. Die Prüfoptionen sind standartisiert, sie können daher nicht geändert werden.

6.5.2. Deaktiviern/Wiederherstellen der Aktivitätsanzeige

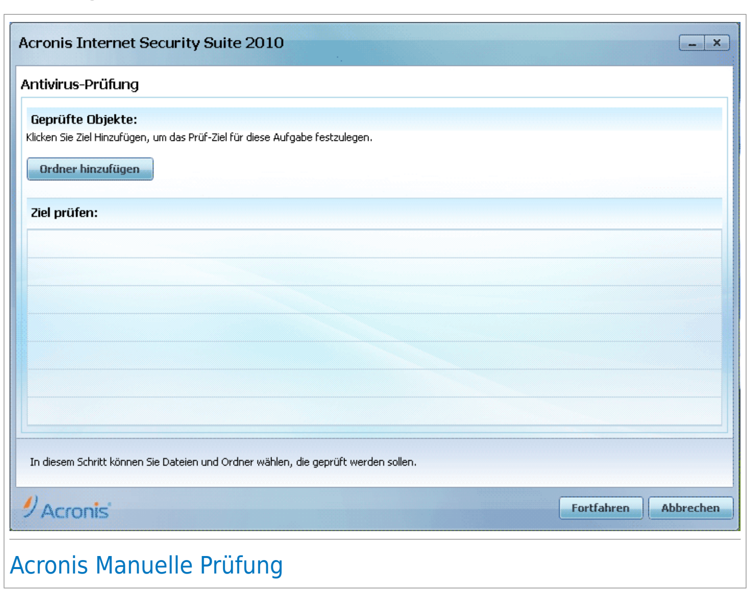
Wenn Sie die graphische Visualisierung nicht länger sehen wollen, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Ausblenden**. Um die Aktivitätsanzeige wiederherzustellen folgen Sie diesen Schritten:

1. Öffnen Sie Acronis Internet Security Suite 2010.
2. Klicken Sie oben rechts im Fenster den **Einstellungen** Schalter.
3. Wählen Sie in der Kategorie Allgemeine Einstellungen das entsprechende Kästchen für die **Aktivitätsanzeige** aus.
4. Klicken Sie **OK**, um die Änderungen zu speichern und zu übernehmen.

6.6. Acronis Manuelle Prüfung

Acronis manuelle Prüfung lässt sie eine Prüfung eines bestimmten Ordners oder einer Festplattenpartition durchführen ohne das Erstellen einer Prüfaufgabe. Diese Funktion wurde implimentiert zur Verwendung im abgesicherten Modus von Windows. Falls Ihr System mit einem anpassungfähigen Virus infiziert wurde, so können Sie versuchen diesen zu entfernen indem Sie Windows im abgesicherten Modus starten und mit der manuellen Prüfung von Acronis jede Festplattenpartition scannen.

Um die Acronis Manuelle Prüfung zu starten, verwenden Sie das Startmenü: **Start** → **Programme** → **Acronis Internet Security Suite 2010** → **Acronis Manuelle Prüfung**. Das folgende Fenster wird erscheinen:



Acronis Manuelle Prüfung

Klicken Sie auf **Ordner hinzufügen**, wählen Sie dann das Ziel dass geprüft werden soll, und wählen Sie **OK**. Wenn Sie mehrere Ordner prüfen möchten, wiederholen Sie diese Aktion für jedes zusätzliches Ziel.

Der Pfad der ausgewählten Position wird in der Spalte **Pfad** angezeigt. Wenn Sie die ausgewählte Position ändern möchten, klicken Sie einfach auf die nebenstehende Schaltfläche **Entfernen**. Klicken Sie auf **Alle entfernen** um alle Ziele die hinzugefügt worden sind, zu löschen.

Wenn Sie fertig sind, klicken Sie **Continue**. Der Antivirusprüfassistend wird erscheinen und Sie durch den Prüfprozess führen. Weitere Informationen zu diesem Assistenten finden Sie unter *„Antivirus Prüfassistent“* (S. 44).

Scanoptionen. Die Prüfoptionen sind für bestmögliche Enteckungsraten vorkonfiguriert. Falls infizierte Dateien entdeckt werden wird Acronis Internet Security Suite 2010 versuchen diese zu desinfizieren (den Mailwarecode entfernen). Wenn die Desinfizierung fehlschlagen sollte wird Ihnen der Antivirus Prüfassistent andere Möglichkeiten anbieten wie mit den infizierten Dateien verfahren werden kann. Die Prüfoptionen sind standartisiert, sie können daher nicht geändert werden.

Was ist Abgesichertes Modus?
Der abgesicherte Modus ist eine Sonderfunktion von Windows, welche in den meisten Fällen zur Behebung von Problemen, die normale Operationen von Windows beeinflussen, verwendet wird. Solche Probleme reichen von Treiberkonflikten, bishin zu Viren welche Windows am normalen Starten hindern. Im abgesicherten Modus lädt Windows nur die nötigsten Betriebssystemkomponenten und Basistreiber. Nur wenige Anwendungen funktionieren im abgesicherten Modus. Das ist der Grund warum die meisten Viren im abgesicherten Modus inaktiv und somit einfach zu entfernen sind.
Um Windows im abgesicherten Modus zu starten, starten Sie ihren Rechner neu und drücken die F8 Taste bis das Windows Erweiterte Optionen Menu erscheint. Sie können zwischen mehreren Optionen wählen. Sie können **abgesicherter Modus mit Netwerktreibern wählen** um auch Internetzugriff zu haben.



Anmerkung

Um mehrere Informationen über Abgesichertes Modus herauszufinden, öffnen Sie die Windows Hilfe/Support (Klicken Sie im Startmenu auf **Hilfe und Support**). Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.

6.7. Spiele-Modus und Laptop-Modus

Einige Computeraktivitäten, wie Spiele oder Presentationen, benötigen erhöhte Ansprechbarkeit und Leistung ohne Unterbrechungen. Wenn Ihr Laptop auf Batteriebetrieb läuft ist es ratsamer unnötige Vorgänge, welche zusätzlich Strom verbrauchen, zu verschieben bis der Laptop extern mit Strom versorgt wird.

Um sich diesen besonderen Situationen anzupassen, hat Acronis Internet Security Suite 2010 zwei spezielle Betriebsmodi:

- Spiele-Modus
- Laptop-Modus

6.7.1. Spiele-Modus

Der Spiele-Modus ändert die Schutzeinstellungen zeitweise, dass ihr Einfluss auf die Leistungsfähigkeit des Systems so gering wie möglich ist. Wenn Sie den Spiele-Modus aktivieren, werden folgende Einstellungen angewendet:

- Berechnungszeit & Speicherverbrauch minimieren
- Automatische Updates & Prüfungen hinausschieben
- Alle Benachrichtigungen und Pop-Ups deaktivieren
- Nur die wichtigsten Dateien prüfen

Wenn der Spiele-Modus aktiviert ist, sehen Sie den Buchstaben G über dem Acronis Symbol.

Spiele-Modus benutzen

Standardmäßig wechselt Acronis Internet Security Suite 2010 automatisch in den Spielemodus, wenn Sie ein Spiel aus der Liste bekannter Spiele starten oder wenn eine Anwendung in die Vollbilddarstellung geht. Acronis Internet Security Suite 2010 wird selbstständig zum Normalbetriebsmodus zurückkehren wenn Sie das Spiel verlassen oder die erkannte Anwendung den Vollbildmodus verlässt.

Falls Sie den Spiele-Modus manuell aktivieren möchten, verwenden Sie eine der folgenden Methoden:

- Klicken Sie mit der rechten Maustaste auf das Acronis-Symbol im System-Tray und wählen Sie **Spiele-Modus einschalten**.
- Drücken Sie `Strg+Shift+Alt+G` (Standard-Tastenkombination)



Wichtig
Vergessen Sie nicht den Spiele-Modus später wieder auszuschalten. Befolgen Sie dazu die selben Schritte wie zum Einschalten des Spiele-Modus.

Tastenkombination für Spiele-Modus ändern

Wenn Sie die Tastenkombination ändern möchten, befolgen Sie folgende Schritte:

1. Öffnen Sie Acronis Internet Security Suite 2010 und wechseln Sie in die Profi-Ansicht.
2. Klicken Sie auf **Spiele-/Laptop- Modus** in dem linken Menü.
3. Klicken Sie auf den Tab **Spiele-Modus**.

4. Klicken Sie auf die Schaltfläche **Weitere Einstellungen**.
5. Wählen Sie die gewünschte Tastenkombination unter der Option **Tastenkombination aktivieren** :
   - Wählen Sie die Tastenkombination die Sie verwenden möchten indem Sie folgende Tasten markieren : Steuerung (`Strg`), Shift (`Shift`) oder Alt-Taste (`Alt`).
   - Geben Sie im Editierfeld die Taste ein, die Sie benutzen möchten.

   Wenn Sie beispielsweise die Tastenkombination `Strg+Alt+D` benutzen möchten, markieren Sie `Strg` und `Alt` und geben Sie `D` ein.

   Anmerkung
   Wenn Sie die Markierung neben **Tastenkombination aktivieren** entfernen, wird die Tastenkombination deaktiviert.

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

6.7.2. Laptop-Modus

Der 'Laptop-Modus' wurde speziell für Laptop- und Notebook-Benutzer entwickelt. Sein Zweck liegt darin, den Einfluss von Acronis Internet Security Suite 2010 auf den Stromverbrauch bei Batteriebetrieb zu minimieren. Im Laptop-Modus werden keine geplanten Prüfungen durchgeführt, da diese mehr Systemresourcen benötigen und dies den Stromverbrauch erhöht.

Acronis Internet Security Suite 2010 erkennt wenn Ihr Laptop über ein Akku läuft und startet den Laptop-Modus automatisch. Ebenso beendet Acronis Internet Security Suite 2010 automatisch den Laptop-Modus, wenn erkannt wird dass der Laptop nicht mehr über einen Akku betrieben wird.

Folgen Sie diesen Schritten, um den Laptop-Modus von Acronis Internet Security Suite 2010 zu aktivieren:

1. Öffnen Sie Acronis Internet Security Suite 2010.
2. Klicken Sie oben rechts im Fenster den **Einstellungen** Schalter.
3. Wählen Sie in der Kategorie Allgemeine Einstellungen das entsprechende Kästchen für die **Laptop-Modus Erkennung** aus.
4. Klicken Sie **OK**, um die Änderungen zu speichern und zu übernehmen.

6.8. Automatische Geräteerkennung

Wenn ein externes Speichergerät mit dem PC verbunden wird, erkennt Acronis Internet Security Suite 2010 dies automatisch, und bietet an, es vor dem Zugriff auf desses Daten, zu prüfen. Dies ist empfohlen um die Infizierung Ihres Systems durch Viren und andere Malware zu verhindern.

Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs
- USB-Speichergeräte, sowie Flashstifte und externe Festplatten
- verbundene (entfernte) Netzlaufwerke

Wenn solch ein Gerät entdeckt wird, erscheint ein Hinweis.



- neues Gerät

Um das Speichergerät zu prüfen, klicken Sie **Ja**. Der Antivirusprüfassistend wird erscheinen und Sie durch den Prüfprozess führen. Weitere Informationen zu diesem Assistenten finden Sie unter *„Antivirus Prüfassistent“* (S. 44).

Falls Sie das Gerät nicht prüfen möchten, klicken Sie **Nein**. In diesem Fall, könnte eine der folgenden Optionen helfen:

- **Bei diesem Gerätetyp nicht mehr nachfragen** - Acronis Internet Security Suite 2010 wird für diesen Gerätetyp keine Prüfung anbieten, wenn dieser mir dem PC verbunden wird.
- **Automatische Geräteerkennung deaktivieren** - Sie werden nicht länger aufgefordert neue Speichergeräte zu prüfen, wenn diese mit dem PC verbunden werden.

Falls Sie die automatische Geräteerkennung versehentlich deaktivieren und sie reaktivieren, oder die Einstellungen anpassen möchten, folgen Sie diesen Schritten:

1. Öffnen Sie Acronis Internet Security Suite 2010 und wechseln Sie in die Profi-Ansicht.
2. Gehen Sie zu **Antivirus>Virusprüfung**.
3. Suchen Sie aus der Liste der Prüfaufgaben **Geräteerkennungsprüfung** heraus.
4. Rechtsklicken Sie die Aufgabe und wählen **Öffnen**. Ein neues Fenster wird sich öffnen.
5. Im **Übersichts** Tab, konfigurieren Sie die Prüfoptionen nach Bedarf. Weitere Informationen finden Sie unter *„Konfigurieren der Prüfoptionen“* (S. 128).
6. Im **Erkennungs** Tab, wählen Sie welche Art von Speichergerät erkannt werden soll.
7. Klicken Sie **OK**, um die Änderungen zu speichern und zu übernehmen.

7. Alle beheben

Acronis Internet Security Suite 2010 benutzt ein Problem-Tracking-System, um sicherheitsgefährdende Probleme festzustellen und Sie über diese zu informieren. Standardmässig werden nur die wichtigsten Bereiche überwacht. Sie können es jedoch so konfigurieren, dass Sie über die von Ihnen gewählten Probleme benachrichtigt werden.

So werden Sie über noch ausstehende Risiken benachrichtigt:

- Um noch ausstehende Risiken anzuzeigen wird ein besonderes Symbol über dem Acronis Symbol im System Tray dargestellt.

  Rotes Dreieck mit einem Ausrufezeichen: Kritische Probleme betreffen die Sicherheit Ihres Systems. Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden.

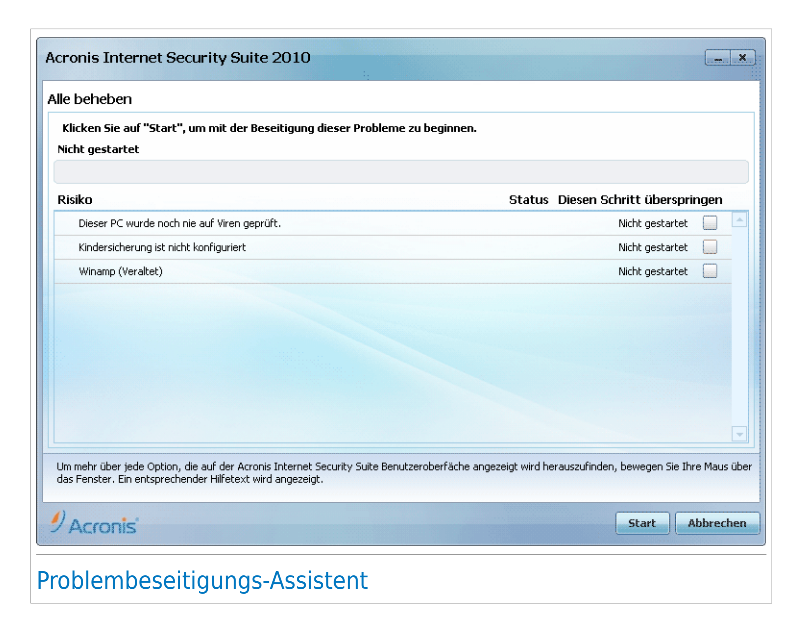
  Wenn Sie den Mauszeiger über das Symbol bewegen, wird Ihnen angezeigt, dass ein Porblem existiert.

- Wenn Sie Acronis Internet Security Suite 2010 öffnen, wird der Bereich Sicherheitsstatus Ihnen die Anzahl der offenen Probleme anzeigen, die Ihr System betreffen.
  - In der Standard-Ansicht, wird der Sicherheitsstatus auf dem **Dashboard** angezeigt.
  - In der Profi-Ansicht, gehen Sie zu **General>Dashboard**, um den Sicherheitsstatus zu prüfen.

7.1. Problembeseitigungs-Assistent

Der einfachste Weg existierende Probleme zu beseitigen, ist Schritt für Schritt dem **Problembeseitigungs-Assistenten** zu folgen. Der Assistent hilft Ihnen alle Bedrohungen Ihres Computers und Ihrer Daten zu beseitigen. Befolgen Sie eine der folgenden Möglichkeiten, den Assistenten zu öffnen:

- Rechtsklicken Sie das Acronis Symbol im System Tray und wählen **Alle beheben**.
- Öffnen Sie Acronis Internet Security Suite 2010. Abhängig vom Benutzeroberflächen-Modus, gehen Sie wie folgt vor:
  - In der Basis-Ansicht, klicken Sie **Alle Probleme beheben**.
  - In der Standard-Ansicht, gehen Sie zum **Dashboard** und klicken Sie **Alle Probleme beheben**.
  - In der Profi-Ansicht, gehen Sie zu **General>Dashboard** und klicken Sie **Alle Probleme beheben**.



Problembeseitigungs-Assistent

Der Assistent zeigt eine Liste der Bedrohungen auf Ihrem Computer an.

All aktuellen Probleme sind zum Beheben ausgewählt. Wenn es ein Problem gibt, dass nicht behoben werden soll, wählen Sie die entsprechende Markierung. Wenn Sie dies tun, wird der Status zu **Überspringen** wechseln.



Anmerkung

Falls Sie über bestimmte Risiken nicht benachrichtigt werden möchten, müssen Sie das Überwachungssystem so konfigurieren wie im nächsten Abschnitt beschrieben.

Um die ausgewählten Risiken zu beheben, klicken Sie auf **Beheben**. Einige Risiken werden sofort behoben.Für die anderen, hilft Ihnen ein Assistent diese zu beheben.

Die Risiken die Ihnen dieser Assistent hilft zu beheben, können in diese Hauptkategorien eingeordnet werden

- **Deaktivierte Sicherheitseinstellungen.** Solche Probleme werden sofort beseitigt, durch die entsprechenden Sicherheitseinstellungen.
- **Vorbeugende Sicherheitsaufgaben die Sie durchführen sollten.** Ein Beispiel für eine solche Aufgabe ist das Prüfen Ihres PC's. Es ist empfohlen dies zumindest einmal wöchentlich zu tun. In den meisten Fällen wird Acronis Internet Security Suite 2010 dies automatisch erledigen. Falls sie die Prüfplanung verändert haben oder diese nicht vollständig ist, so werden Sie darüber informiert werden.

  Bei der beseitigung solcher Probleme, hilft Ihnen ein Assistent.

- **System Schwachstellen.** Acronis Internet Security Suite 2010 untersucht automatisch Ihr System nach Schwachstellen und warnt Sie. Systemschwachstellen beinhalten das Folgende:
  - ▶ Schwache Windows Benutzerkonten Passwörter.
  - ▶ Nicht aktuelle Software auf Ihrem PC.
  - ▶ fehlende Windows Updates.
  - ▶ Automatisches Windows Update ist deaktiviert.

  Wenn solche Probleme beseitigt werden sollen, startet der Schwachstellen-Prüfungsassistent. Der Assistent hilft Ihnen bei der Beseitigung der entdeckten Schwachstellen. Weitere Informationen finden Sie unter „*Schwachstellenprüfassistent*“ (S. 56).

7.2. Konfigurieren der Problem-Verfolgung

Das Risikoüberwachungssystem ist vorkonfiguriert die wichtigsten Risiken die die Sicherheit Ihres Systems und Daten gefährden zu überwachen und Sie darüber zu informieren . Weitere Risiken werden überwacht basierend auf der getroffenen Auswahl im Konfigurationsassistenten (wenn Sie ihr Benutzerprofil festlegen). Neben den überwachten standard Problemen, gibt es weitere, über die Sie sich informieren lassen können.

Sie können das Tracking System so konfigurieren, dass es Ihren Sicherheitsansprüchen gerecht wird, indem Sie besondere Punkte auswählen, über die Sie informiert werden möchten. Dies können Sie sowohl in der Standard- als auch im Profi-Ansicht machen.

- In der Standard-Ansicht kann das Tracking System auf verschiedene Weise konfiguriert werden. Folgen Sie diesen Schritten:
  1. Klicken Sie auf **Sicherheit**, **Eltern** oder **Datentresor** Tab.
  2. Klicken Sie auf **Konfiguriere Status Warnungen**.
  3. Markieren Sie die Kästchen der Punkte, die überwacht werden sollen.

  Für weitere Informationen lesen Sie bitte „Standard-Ansicht“ (S. 82) diesen Teil des Benutzerhandbuchs.

- In der Profi-Ansicht kann das Tracking System zentral konfiguriert werden. Folgen Sie diesen Schritten:
  1. Gehen Sie auf **General>Dashboard**.
  2. Klicken Sie auf **Konfiguriere Status Warnungen**.
  3. Markieren Sie die Kästchen der Punkte, die überwacht werden sollen.

  Für weitere Informationen lesen Sie bitte „*Dashboard* “ (S. 104).

8. Konfigurieren der Grundeinstellungen

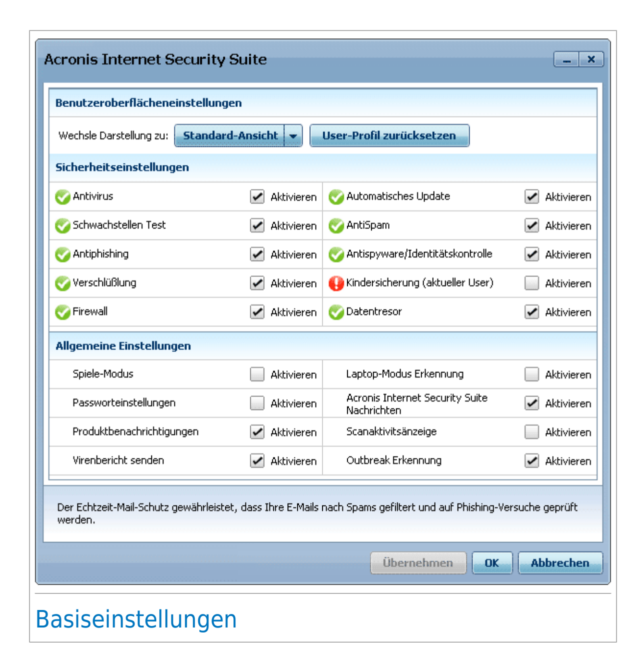
Sie können die Haupteinstellungen des Produkts (einschliesslich der Benutzeransicht) vom Fenster der Grundeinstellungen aus konfigurieren. Um es zu öffnen, tun Sie das Folgende:

- Öffen Sie Acronis Internet Security Suite 2010 und klicken Sie **Einstellungen** am oberen, rechten Rand des Fensters.
- Sie können das Acronis Icon im system tray rechts-klicken und **Basiseinstellungen** wählen.



Anmerkung

Um das Produkt im Detail einzustellen, benutzen Sie die Profi-Ansicht. Weitere Informationen finden Sie unter dem Kapitel „Profi Modus“ (S. 103) in diesem Handbuch.



Basiseinstellungen

Die Einstellungen sind in drei Gruppen unterteilt:

- Benutzeroberflächen- Einstellungen
- Sicherheitseinstellungen
- Allgemeine Einstellungen

Um die Änderungen anzuwenden und zu sichern, klicken Sie **OK**. Um das Fenster zu schliessen ohne die Änderungen zu übernehmen, wählen Sie **Abbrechen**.

8.1. Benutzeroberflächeneinstellungen

In diesem Bereich können Sie die Benutzeroberfläche-Ansicht und das Nutzprofil zurücksetzen.

Die Ansicht der Bedienoberfläche wird umgeschaltet. Wie beschrieben in Abschnitt *„Benutzeroberfläche Ansichtsmodus“* (S. 12), gib es drei Modi zur Anzeige der Benutzeroberfläche. Jeder Modus ist für eine bestimmte Benutzergruppe ausgelegt, abhängig von ihren Computerkenntnissen. So wird die benutzeroberfläche allen Arten von Anwendern gerecht, von Computer Neulingen bis hin zu Technikern.

Die erste Schaltfläche zeigt die aktuelle Benutzeroberfläche. Um die Benutzeroberflächen-Ansicht zu ändern, klicken Sie den Pfeil und wählen Sie den gewünschten Modus.

Modus	Beschreibung
Basis-Ansicht	Geeignet für Anfänger und für diejenigen, die Acronis Internet Security Suite 2010 ohne Aufwand zum Schutz ihres Computers und ihrer Daten nutzen wollen. Diese Ansicht ist einfach in der Handhabung und verlangt minimalen Aufwand Ihrerseits. Sie müssen nur die existierenden Punkte beheben, wenn Acronis Internet Security Suite 2010 Sie dazu auffordert. Ein intuitiver Schritt für Schritt Assistent hilft Ihnen dabei. Zusätzlich können Sie gewöhnliche Aufgaben ausführen, wie das Aktualisieren der Acronis Internet Security Suite 2010 Virensignaturen und Produktdateien oder die Prüfung Ihres Computers.
Standard-Ansicht	Für Benutzer mit durchschnittlicher Computer-Erfahrung, erweitert diese Ansicht die Basis-Einstellungen. Sie können offene Punkte separat beheben und wählen welche Punkte überwacht werden. Ferner können Sie die Acronis Produkte auf entfernten Computern in Ihrem Haushalt verwalten.
Profi-Ansicht	Für technisch fortgeschrittene Anwender, erlaubt Ihnen diese Ansicht jede Funktion von Acronis Internet Security Suite 2010 zu konfigurieren. Sie können auch alle Funktionen benutzen, um Ihren Computer und Ihre Daten zu schützen.

Die Benutzerprofile rekonfigurieren. Das Nutzungsprofil reflektiert die hauptsächlich durchgeführten Aktivitäten auf dem Computer. Abhängig von

Nutzungsprofil, wird die Benutzeroberfläche sortiert, damit Sie bequem auf Ihre bevorzugten Aufgaben zugreifen können.

Klicken Sie zur Rekonfiguration des Benutzerprofils auf **Profil rekonfigurieren** und folgen Sie dem Konfigurationsassistenten.

8.2. Sicherheitseinstellungen

Hier können Sie Einstellungen aktivieren/deaktivieren, die verschiedene Bereiche von Computer und Datensicherheit betreffen. Der aktuelle Status einer Einstellung wird durch eine dieser Symbole dargestellt:

Grüner Kreis mit einem Häkchen: Die Einstellung ist aktiviert.

Roter Kreis mit einem Ausrufezeichen: Die Einstellung ist deativiert.

Um eine Einstellung zu aktivieren/deaktivieren, setzen/löschen Sie das Häkchen in dem **Aktivieren** Feld.



Warnung

Wir raten Ihnen zur Vorsicht wenn Sie den Echtzeitschutz, Firewall oder das automatische Update deaktivieren. Diese Funktionen zu deaktivieren kann die Sicherheit Ihres Computers gefährden. Falls sie wirklich einmal deaktiviert werden müssen, vergessen Sie nicht sie so bald als möglich zu reaktivieren.

Die Liste der Einstellungen und Ihrer Beschreibung wird in der folgenden Tabelle dargestellt:

Einstellung	Beschreibung
Antivirus	Der Echtzeit-Dateischutz gewährleistet, dass alle Dateien geprüft werden, sobald auf sie zugegriffen wird, sei es durch Sie oder eine ausgeführte Anwendung.
Automatisches Update	Durch das automatische Update werden die aktuellsten Acronis Internet Security Suite 2010 Produkt-Dateien und Signaturen regelmäßig und automatisch heruntergeladen und installiert.
Schwachstellenprüfung	Die automatische Schwachstellenprüfung gewährleistet, dass wichtige Software auf Ihrem PC stets auf dem neusten Stand ist.
Antispam	Antispam filtert die eingehenden E-Mails und markiert unerwünschte und Junk-Mails als SPAM.
Antiphishing	Antiphishing entdeckt und alamiert sie umgehend in Echtzeit wenn eine Webseite dazu konfiguriert ist persönliche Informationen zu stehlen.

Einstellung	Beschreibung
Identitätskontrolle	Die Indentitätskontrolle verhindert, dass persönliche Daten ohne Ihr Einverständnis ins Internet gesendet werden. Es blockiert IM Nachrichten, E-Mail oder online Mail die Daten an dritte senden wollen, die Sie als privat definiert haben.
IM-Verschlüsselung	IM (Instant Messaging) Verschlüsselung sichert Ihre Unterhaltungen im Yahoo! Messenger und Windows Messenger, vorausgesetzt, dass Ihr IM Kontakt ebenfalls ein kompatibles Acronis Produkt und IM Software benutzt.
Kindersicherung	Kindersicherung begrenzt die Rechner- und Online-Aktivitäten Ihrer Kinder, basierend auf die von Ihnen festgelegeten Regeln. Beschränkungen können das Blockieren von unsachgemässen Web-Seiten beinhalten, sowie begrenzten Spiele- und Internet-Zugriff gemäss des festgelegten Zeitplans.
Firewall	Die Firewall schützt Ihren Computer vor Hackern und schädlichen Angriffen.
Datei-Verschlüsselung	Der Dateischutz schützt Ihre Dokumente indem diese in besonders geschützten Laufwerken verschlüsselt werden Wenn Sie den Dateischutz deaktivieren, wird jeder Dateischutz abgeschlossen und Sie haben keinen Zugriff mehr auf die sich darin befindenden Dateien.

Der Status von einigen dieser Einstellungen kann durch das Acronis Internet Security Suite 2010 Tracking-System überwacht werden. Wenn Sie eine überwachte Einstellung deaktivieren, zeigt Acronis Internet Security Suite 2010 dieses als Risiko an, die Sie beheben müssen.

Wenn Sie nicht wollen, dass eine überwachte Einstellung als ein Problem angezeigt wird, müssen Sie das Tracking System entsprechend konfigurieren. Das können Sie entwerder in der Standard-Ansicht oder Profi-Ansicht.

- In der Zwischen-Ansicht kann das Tracking System auf verschiedene Weise konfiguriert werden. Für weitere Informationen lesen Sie bitte „Standard-Ansicht“ (S. 82) diesen Teil des Benutzerhandbuchs.
- In der Profi-Ansicht kann das Tracking System zentral konfiguriert werden. Folgen Sie diesen Schritten:
  1. Gehen Sie auf **General>Dashboard**.
  2. Klicken Sie auf **Konfiguriere Status Warnungen**.
  3. Entfernen Sie die Markierung des Objektes, dass nicht beobachtet werden soll.

Für weitere Informationen lesen Sie bitte *„Dashboard "* (S. 104).

8.3. Allgemeine Einstellungen

In diesem Berecih können Sie Einstellungen aktivieren/deaktivieren, die das Produktverhalten beeinflussen. Um eine Einstellung zu aktivieren/deaktivieren, setzen/löschen Sie das Häkchen in dem **Aktivieren** Feld.

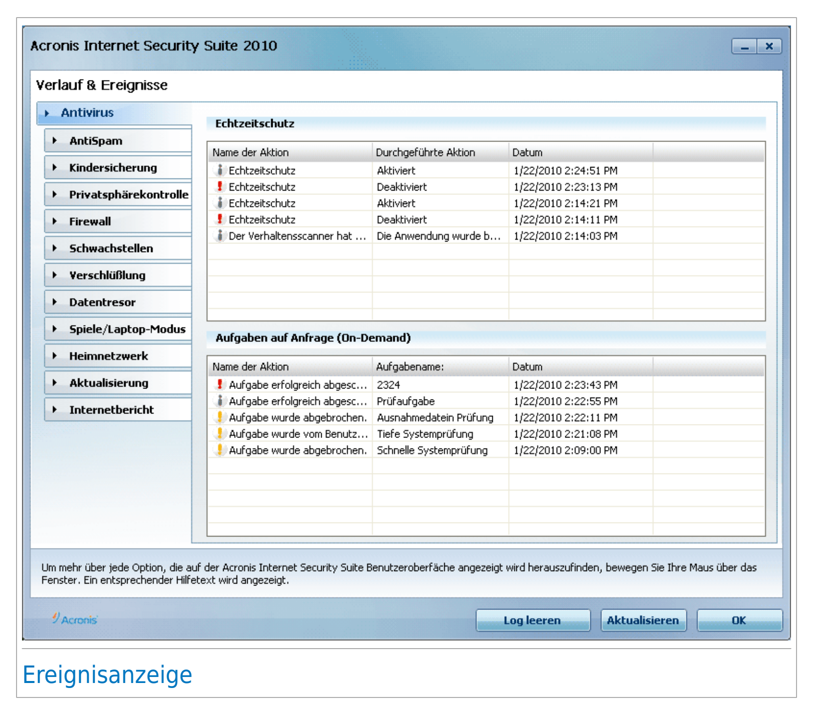
Die Liste der Einstellungen und Ihrer Beschreibung wird in der folgenden Tabelle dargestellt:

Einstellung	Beschreibung
Spiele-Modus	Der Spiele-Modus verändert temporär die Einstellungen so, dass die Systemleistung während des Spielens so wenig wie möglich beeinträchtigt wird.
Laptop-Modus	Der Laptop-Modus verändert temporär die Einstellungen, so dass die Betriebsdauer des Laptopakkus so wenig wie möglich beeinträchtigt wird.
Passwort für Einstellungen	Dies gewährleistet, dass die Einstellungen von Acronis Internet Security Suite 2010 nur von der Person verändert werden können, die das Passwort kennt. Wenn Sie diese Option aktivieren, werden SIe aufgefordert das Einstellungspasswort zu erstellen. Geben Sie das Passwort in beide Felder ein und klicken Sie auf **OK** um das Passwort fest zu legen.
Acronis Internet Security Suite Nachrichten	Wenn Sie diese Option aktivieren, erhalten Sie von Acronis wichtige Firmenneuigkeiten, Produkt-Updates oder Informationen über die neusten Sicherheitsbedrohungen.
Produktbenachrichtigungen	Wenn Sie diese Option aktivieren, erhalten Sie Informationsbenachrichtigungen.
Aktivitätsleiste	Die Aktivitätsanzeige ist ein kleines, transparentes Fenster welches den Verlauf von Acronis Internet Security Suite 2010 Prüfaktivitäten anzeigt. Für weitere Informationen lesen Sie bitte*„Scanaktivitsänzeige"* (S. 27).
Virenbericht senden	Wenn Sie diese Option aktivieren, werden Virenberichte zum Acronis Labor für weitere Analysen gesendet. Bitte beachten Sie, dass diese Berichte keine vertraulichen Daten, wie Ihren Namen oder Ihre IP-Adresse enthalten und nicht für kommerzielle Zwecke verwendet werden.

Einstellung	Beschreibung
Ausbruchentdeckung	Wenn Sie diese Option aktivieren, werden Berichte über einen möglichen Virenausbruch zum Acronis Labor für weitere Analysen gesendet. Bitte beachten Sie, dass diese Berichte keine vertraulichen Daten, wie Ihren Namen oder Ihre IP-Adresse enthalten und nicht für kommerzielle Zwecke verwendet werden.

9. Verlauf und Ereignisse

Der Link **Protokolle** im unteren Teil des Hauptfensters von Acronis Internet Security Suite 2010 öffnet ein weiteres Fenster mit Verlauf & Ereignissen von Acronis Internet Security Suite 2010. Dieses Fenster bietet Ihnen einen Überblick zu sicherheitsbezogenen Ereignissen. So können Sie beispielsweise einfach überprüfen ob das Update erfolgreich durchgeführt wurde, ob Malware auf Ihrem entdeckt wurde usw.



Ereignisanzeige

Um eine gute Übersicht zu gewähren wurden die Acronis Internet Security Suite 2010 Ereignise auf der linken Seite in verschiedene Gruppen aufgeteilt:

- **Antivirus**
- **Antispam**
- **Kindersicherung**
- **Privatsphäre**
- **Firewall**
- **Schwachstellen**
- **IM-Verschlüsselung**
- **Datei-Verschlüsselung**

- **Spiele-/Laptop-Modus**
- **Heim Netzwerk**
- **Update**
- **Internet Log**

Für jede Kategorie ist eine Liste von Ereignisen verfügbar. Jedes Ereignis enthält folgende Informationen: Eine Kurzbeschreibung, die von Acronis Internet Security Suite 2010 durchgeführte Aktion, sowie Datum und Zeitpunkt des Auftretens. Wenn Sie nähere Informationen zu einem Ereignis erhalten möchten dann klicken Sie doppelt auf selbiges.

Klicken Sie auf **Zurücksetzen** wenn Sie die Einträge entfernen möchten oder auf **Aktualisieren** um sicherzustellen das die Anzeige aktuell ist.

10. Assistent

Um die Bedienung von Acronis Internet Security Suite 2010 zu vereinfachen, helfen Ihnen mehrere Assistenten dabei bestimmte Sicherheits-Aufgaben durchzuführen oder komplexere Einstellungen vorzunehmen. Dieses Kapitel beschreibt den Assistenten, der erscheint, wenn Probleme zu beheben, oder besondere Aufgaben mit Acronis Internet Security Suite 2010 durchzuführen sind. Andere Konfigurationsassistenten werden separat beschrieben im „Profi Modus“ (S. 103) Teil.

10.1. Antivirus Prüfassistent

Wann immer Sie den On-Demand Scan einleiten (z.B, Rechtsklick auf einen Ordner und dor wählen **Scanne mit Acronis Internet Security Suite**), wird der Antivirus Prüfassistent erscheinen. Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.



Anmerkung

Falls der Prüfassistent nicht erscheint, ist die Prüfung möglicherweise konfiguriert still, im Hintergrund, zu laufen. Sehen Sie nach dem Prüffortschritticon im Systemtray. Sie können dieses Objekt anklicken um das Prüffenster zu öffnen und so den Prüffortschritt zu sehen.

10.1.1. Schritt 1/3 - Prüfvorgang

Acronis Internet Security Suite 2010 prüft die gewählten Dateien und Ordner.



Prüfvorgänge durchführen

Sie können den Vorgangsstatus und die Statistiken hierzu sehen (Prüfgeschwindigkeit, vergangene Zeit, Anzahl der geprüften / infizierten / verdächtigen / versteckten Objekte).

Warten Sie bis Acronis Internet Security Suite 2010 den Prüfvorgang beendet hat.



Anmerkung

Der Prüfvorgang kann, abhängig von der Größe Ihrer Festplatte, einen Moment dauern.

Passwortgeschützte Archive. Wenn Acronis Internet Security Suite 2010 während des Prüfvorgangs ein passwortgeschütztes Archiv entdeckt und die Standartaktion ist **Frage nach Passwort**, Sie werden aufgefordert das Passwort anzugeben. Mit Passwörtern geschützte Archive können nicht geprüft werden, außer wenn Sie das Passwort angeben. Die folgenden Optionen sind verfügbar:

- **Ich möchte für dieses Objekt das Passwort eingeben.** Wenn Sie möchten das Acronis Internet Security Suite 2010 Archive prüftt, wählen Sie diese Option aus und geben das Passwort an. Falls Sie das Passwort nicht kennen, wählen Sie eine der anderen Optionen.
- **Ich möchte für dieses Objekt kein Passwort angeben (dieses Objekt überspringen).** Wählen Sie diese Optione um das Prüfen diesen Archivs zu überspringen.

- **Ich möchte für kein Objekt ein Passwort angeben (alle passwortgeschützten Objekte überspringen).** Wählen Sie diese Option, falls Sie nicht über passwortgeschützte Archive informiert werden möchten. Acronis Internet Security Suite 2010 wird nicht in der Lage sein sie zu prüfen, jedoch wird eine Aufzeichnung im Prüflog eingetragen.

Klicken Sie auf **OK** um fortzufahren.

Stoppen oder pausieren der Prüfung. Sie können den Prüfvorgang jederzeit durch einen Klick auf **Stop&Ja** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten. Um den Prüfvorgang vorrübergehend zu stoppen klicken Sie einfach auf **Pause**. Um den Prüfvorgang fortzusetzen klicken Sie auf **Fortsetzen** .

10.1.2. Schritt 2/3 - Aktionsauswahl

Wenn der Prüfvorgang beendet wurde wird Ihnen ein Fenster angezeigt in welchem Sie eine Zusammenfassung angezeigt bekommen.



Aktionen

Sie bekommen die Anzahl der Risiken welche Ihr System betreffen angezeigt.

Die infizierten Objekte werden in Gruppen angezeigt, je nach Malware, mit der sie infiziert sind. Klicken Sie auf den Link, der der Bedrohung entspricht, um weitere Informationen über die infizierten Objekte zu erhalten.

Sie können eine umfassende Aktion für alle Probleme auswählen oder Sie können einzelne Aktionen für Problemgruppen auswählen.

Eine oder mehrere der folgenden Optionen können im Menu erscheinen:

Aktion	Beschreibung
Keine Aktion durchführen	Es wird keine Aktion für die infizierte Dateien ausgeführt. Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.
Desinfizieren	Den Malware-Code aus den entdeckten infizierten Dateien entfernen.
Löschen	Löscht die infizierten Dateien.
In Quarantäne verschieben	Verschiebt die entdeckten Dateien in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Dateien umbenennen	Die neue Erweiterung der versteckten Dateien wird `.bd.ren` sein. Infolgedessen werden Sie im Stande sein, zu suchen und solche Dateien auf Ihrem Computer zu finden, falls etwa. Bitte beachten Sie das es sich bei den versteckten Dateien nicht um die absichtlich von Windows verborgenen Dateien handelt. Die relevanten sind die von speziellen Programmen versteckten, bekannt als Rootkits. Rootkits sind nicht grundsätzlich schädlich. Jedoch werden Sie allgemein dazu benutzt Viren oder Spyware vor normalen Antivirenprogrammen zu tarnen.

Klicken Sie auf **Fortfahren** um die festgelegten Aktionen anzuwenden.

10.1.3. Schritt 3/3 - Zusammenfassung

Wenn Acronis Internet Security Suite 2010 das Beheben der Risiken beendet hat wird eine Zusammenfassung in einem neuen Fenster geöffnet.



Übersicht

Ihnen wird eine Zusammenfassung angezeigt. Falls Sie umfangreichere Informationen zum Prüfverlauf möchten, klicken Sie **Protokoll** um die Logdatei einzusehen.



Wichtig

Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Säuberungsprozess abgeschlossen werden kann.

Klicken Sie auf **Schließen** um dieses Fenster zu schließen.

Acronis Internet Security Suite 2010 konnte einige Probleme nicht lösen

In den meisten Fällen desinfiziert Acronis Internet Security Suite 2010 erfolgreich die infizierten Dateien, die er entdeckt hat, oder er isoliert die Infektion. Dennoch gibt es Probleme, die nicht gelöst werden können.

In diesen Fällen empfehlen wir Ihnen unser Acronis Support Team unter http://www.acronis.de/support/?ow=1 zu kontaktieren. Die Mitarbeiter unseres Supports werden Ihnen dabei helfen die entsprechenden Probleme zu lösen.

Von Acronis Internet Security Suite 2010 entdeckte verdächtige Dateien

Verdächtige Dateien sind Dateien, die von der heuristischen Analyse als potentiell infiziert erkannt werden, und deren Signaturen noch nicht bekannt sind.

Falls verdächtige Dateien während des Prüfvorganges erkannt werden, werden Sie aufgefordert, diese Dateien zum Acronis-Labor zu senden. Klicken Sie auf **OK** um diese Dateien zum Acronis Lab für weitere Analysen zu senden.

10.2. Prüfassistent anpassen

Der Benutzerdefinierte Prüfassistent lässt Sie eine Prüfaufgabe selbst erstellen und starten, und speichert diese optional auch als Quick Task wenn Sie Acronis Internet Security Suite 2010 in der Mittleren Ansicht verwenden.

Um eine benutzerdefinierte Prüfaufgabe mit Hilfe des Prüfassistenten zu starten folgen Sie diesen Schritten:

1. Gehen Sie in der Mittleren Ansicht auf das **Sicherheits** Tab.
2. In Quick Tasks klicken Sie **Individuelle Prüfung**.
3. Befolgen Sie die sechs Schritt Anleitung um den Prüfvorgang durchzuführen.

10.2.1. Schritt 1/6 - Einführung

Das ist ein Willkommensfenster.



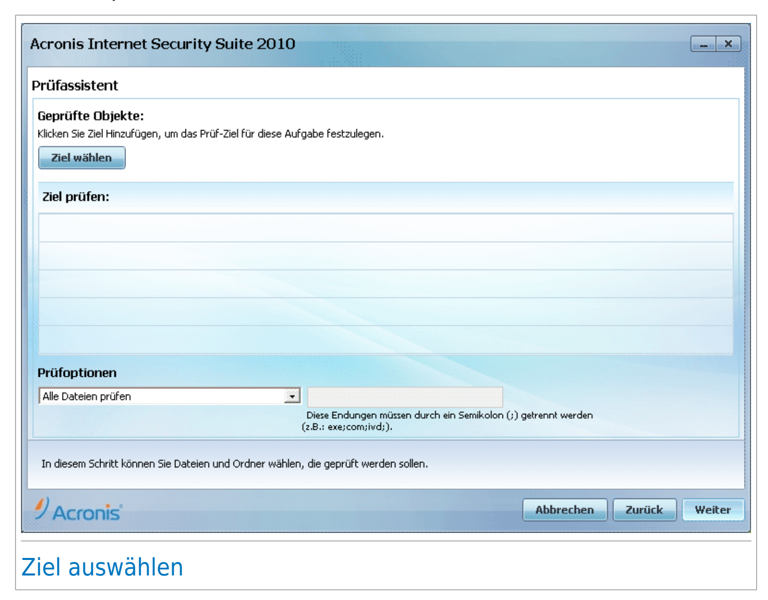
Begrüßungsfenster

Wenn Sie diesen Schritt zukünftig überspringen wollen, wählen Sie **Diesen Schritt nächstes mal nicht mehr anzeigen**.

Klicken Sie auf **Weiter**.

10.2.2. Schritt 2/6 - Ziel auswählen

Hier können Sie die Dateien und Ordner auswählen die geprüft werden sollten sowie die Prüfoptionen.



Ziel auswählen

Klicken Sie auf **Ziel hinzufügen**, wählen Sie dann die Dateien und Ordner die hinzugefügt werden sollen und wählen Sie **OK**. Die dazugehörigen Pfade werden unter **Ziel Prüfen** angezeigt. Wenn Sie die ausgewählte Position ändern möchten, klicken Sie einfach auf die nebenstehende Schaltfläche **Entfernen**. Klicken Sie auf **Alle entfernen** um alle Ziele die hinzugefügt worden sind, zu löschen.

Nachdem Sie den Prüfort ausgewählt haben, legen Sie die **Prüfoptionen** fest. Verfügbar sind die folgenden:

Optionen	Beschreibung
Alle Dateien prüfen	Wählen Sie diese Option, um alle ausgewählten Objekte zu prüfen.
Nur Dateinamenerweiterungen prüfen	Prüft ausschließlich Dateien mit den Dateiendungen: `.exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js;`

Optionen	Beschreibung
	`.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` und `.nws`.
Nur benutzerdefinierte Endungen prüfen	Nur die Dateien werden überprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.

Klicken Sie auf **Weiter**.

10.2.3. Schritt 3/6 – Aktion auswählen

Hier können Sie die Prüfeinstellungen sowie die Prüfstufe wählen.



Aktion auswählen

- Wählen Sie die durchzuführenden Aktionen für entdeckte Dateien die infiziert oder verdächtig sind. Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Keine Aktion durchführen	Es wird keine Aktion für infizierte Dateien ausgeführt. Diese Dateien können Sie in der Berichtsdatei einsehen.

Aktion	Beschreibung
Dateien reparieren	Den Malware-Kode aus den entdeckten infizierten Dateien entfernen.
Dateien löschen	Infizierte Dateien werden ohne Warnung sofort gelöscht.
In die Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

- Wählen Sie die durchzuführende Aktion für die erkannten versteckten Dateien (Rootkits): Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Keine Aktion durchführen	Es wird keine Aktion für versteckte Dateien ausgeführt. Diese Dateien finden Sie in der Berichtsdatei.
Umbenennen	Die neue Erweiterung der versteckten Dateien wird `.bd.ren` sein. Infolgedessen werden Sie im Stande sein, zu suchen und solche Dateien auf Ihrem Computer zu finden, falls etwa.

- Prüfungsaggressivität konfigurieren. 3 Stufen sind wählbar. Verschieben Sie den Regler auf der Skala um die passende Sicherheitsstufe festzulegen:

Scan Level	Beschreibung
Tolerant	Es werden ausschliesslich Anwendungsdateien geprüft und diese auch nur auf Viren. Der Resourcenverbrauch ist niedrig.
Standard	Das Resourcenverbrauchsniveau ist durchschnittlich. Alle Dateien werden auf Viren und Spyware geprüft.
Aggressiv	Alle Dateien (inklusive Archive) werden auf Viren und Spyware geprüft. Versteckte Dateien und Prozesse werden ebenfalls geprüft, der Resourcenverbrauch ist höher.

Fortgeschrittene Anwender möchten womöglich die von Acronis Internet Security Suite 2010 angebotenen Prüfeinstellungen nutzen. Die Prüfung kann festgelegt

werden nur auf bestimmte Malware-Bedrohungen zu suchen. Dies kann Prüfzeiten extrem verkürzen und die PC-Ansprechbarkeit während der Prüfung verbessern.

Setzen Sie den Regler auf **Benutzerdefiniert** und klicken auf die **Angepasste Stufe**-Schaltfläche. Ein neues Fenster wird sich öffnen. Wählen Sie die Art von Malware die Acronis Internet Security Suite 2010 prüfen sollte:

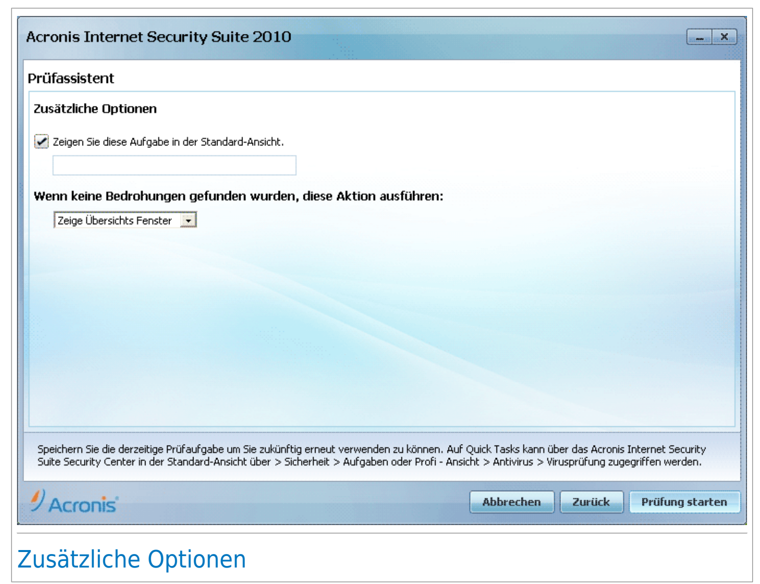
Optionen	Beschreibung
Dateien prüfen	Sucht nach bekannten Viren. Acronis Internet Security Suite 2010 erkennt auch unvollständige Virenkörper, dadurch wird Ihr System zusätzlich geschützt.
Auf Adware prüfen	Sucht nach möglichen Adware-Anwendungen. Entsprechende Dateien werden wie infizierte Dateien behandelt. Software mit Adware-Komponenten arbeitet unter Umständen nicht mehr, wenn diese Option aktiviert ist.
Auf Spyware prüfen	Sucht nach bekannter Spyware. Entsprechende Dateien werden wie infizierte Dateien behandelt.
Anwendungen prüfen	Legitime Anwendungen prüfen, die als Spionage-Tool verwendet werden können, um schädliche Anwendungen oder andere Bedrohungen zu verbergen.
Auf Dialer prüfen	Prüft auf Anwendungen welcher kostenpflichtige Nummern wählen. Erkannte Dateien werden als infiziert behandelt. Dadurch ist es möglich das betroffene Anwendungen nicht mehr funktionsfähig sind.
Auf Rootkits prüfen	Prüft nach versteckten Objekten (Dateien und Prozesse), meist Rootkits genannt.
Auf Keyloggers prüfen	Sucht nach bösartigen Anwendungen, die Tastauranschläge aufzeichnen.

Klicken Sie auf **OK**, um dieses Fenster zu schließen.

Klicken Sie auf **Weiter**.

10.2.4. Schritt 4/6 - Zusätzliche Einstellungen

Es noch zusätzliche Optionen verfügbar, bevor die Prüfung beginnt:



Zusätzliche Optionen

- Um die benutzerdefinierten Aufgaben, die zur späteren Verwendung erstellt werden, zu speichern, wählen Sie **Diese Aufgabe in der Mittleren Ansicht anzeigen** aus, und geben einen Namen für die Regel im angebotenen Feld ein.

  Die Aufgabe wird zur Liste der bereits verfügbaren Quick Tasks im Sicherheits-Tab hinzugefügt und ebenso in der **Profi Ansicht > Antivirus > Virusprüfung** angezeigt.

- Wählen Sie aus dem korrespondierenden Menü eine auszuführende Aktion, sofern keine Bedrohungen gefunden wurden.

Klicken Sie **Prüfung Starten**.

10.2.5. Schritt 5/6 - Prüfen

Acronis Internet Security Suite 2010 prüft die gewählten Dateien und Ordner:



Prüfvorgänge durchführen



Anmerkung

Der Prüfvorgang kann, abhängig von der Größe Ihrer Festplatte, einen Moment dauern. Wenn Sie auf der Prüfvortschrittanzeige sich in system tray befindet wird sich ein Fenseter mit dem Prüfvortschritt öffnen.

10.2.6. Schritt 6/6 - Ergebnisse betrachten

Wenn Acronis Internet Security Suite 2010 den Prüfvorgang beendet hat wird eine Zusammenfassung in einem neuen Fenster geöffnet.



Übersicht

Falls Sie umfangreichere Informationen zum Prüfverlauf möchten, klicken Sie **Protokoll** um die Logdatei einzusehen.



Wichtig

Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Säuberungsprozess abgeschlossen werden kann.

Klicken Sie auf **Schließen** um dieses Fenster zu schließen.

10.3. Schwachstellenprüfassistent

Der Assisten überprüft das System nach Schwachstellen und hilft Ihnen diese zu beheben.

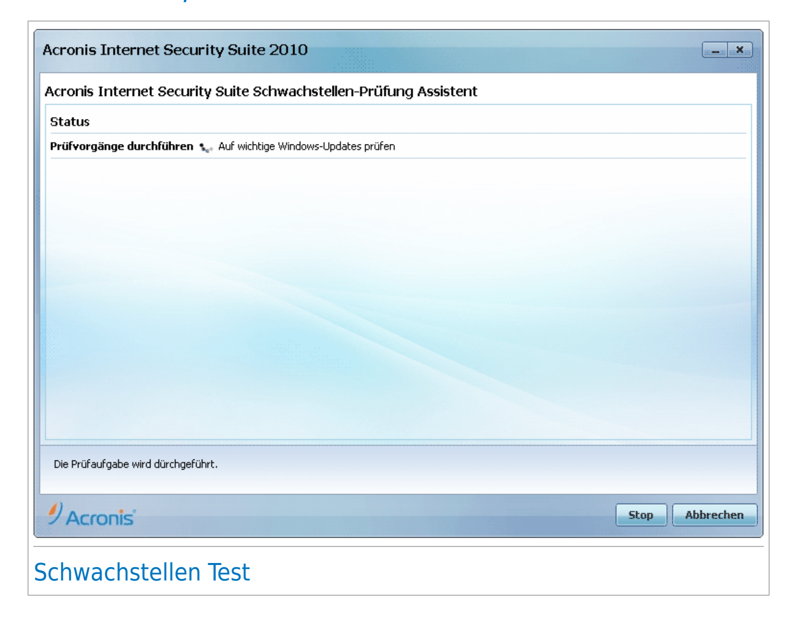
10.3.1. Schritt 1/6 - Auswahl der zu prüfenden Schwachstellen



Schwachstellen

Klicken Sie auf **Weiter** um das System auf die ausgewählten Schwachstellen zu überprüfen.

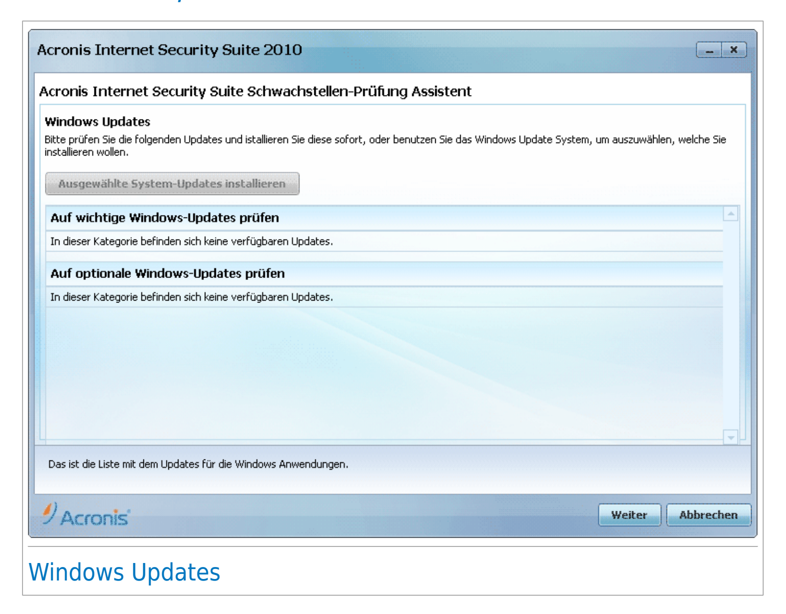
10.3.2. Schritt 2/6 - Nach Schwachstellen suchen



Schwachstellen Test

Bitte warten Sie bis Acronis Internet Security Suite 2010 die Prüfung auf Schwachstellen beendet hat.

10.3.3. Schritt 3/6 - Windows aktualisieren



Windows Updates

Sie können die Liste der wichtigen und weniger wichtigen Windows-Updates sehen, die zur Zeit nicht auf Ihrem Computer installiert sind. Klicken Sie auf **Alle System-Updates installieren**, um die verfügbaren Updates zu installieren.

Klicken Sie auf **Weiter**.

10.3.4. Schritt 4/6 - Anwendungen aktualisieren

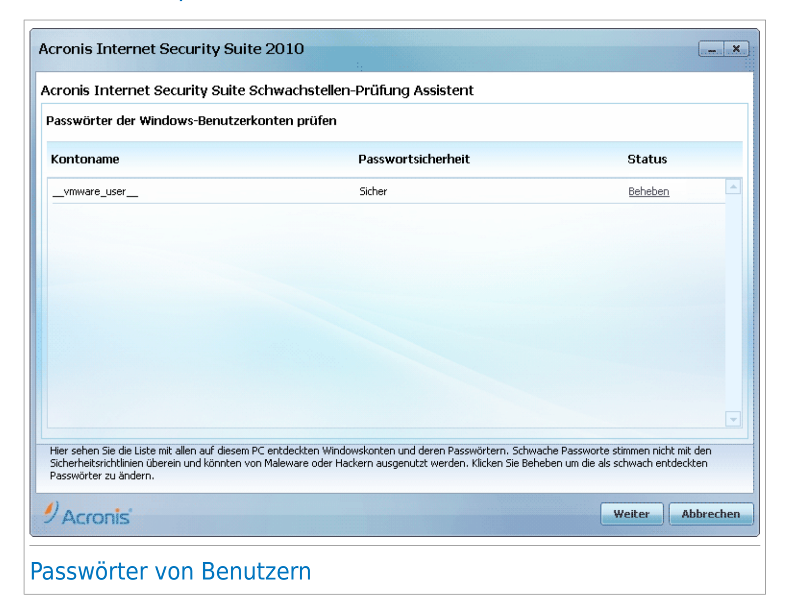


Anwendungen

Sie können eine Liste der Anwendungen sehen, die von Acronis Internet Security Suite 2010 geprüft wurden und ob diese auf dem neusten Stand sind. Wenn eine Anwendung nicht auf dem neusten Stand ist, klicken Sie auf den zur Verfügung stehenden Link um die aktuellste Version herunterzuladen.

Klicken Sie auf **Weiter**.

10.3.5. Schritt 5/6 - Unsicheres Passwort ändern



Passwörter von Benutzern

Sie können die Liste der auf Ihrem Computer konfigurierten Windows-Benutzerkonten sehen und die Sicherheit, die das jeweilige Passwort bietet. Ein Passwort kann **stark**(also schwer herauszufinden) oder **schwach** (also durch Hacker mit Hilfe von speziellen Programmen leicht zu knacken), sein.

Klicken Sie auf **Beheben**, um unsichere Passwörter zu ändern. Ein neues Fenster wird sich öffnen.



Passwort ändern

Wählen Sie die Methode um ein Problem zu beheben:

- **Den Benutzer zwingen das Passwort beim nächsten Login zu ändern.** Beim nächsten Windows-Login wird Acronis Internet Security Suite 2010 den Benutzer dazu auffordern das Passwort zu ändern.
- **Benutzerpasswort ändern.** Geben Sie das neue Passwort in jedes der Editierfelder ein. Stellen Sie sicher den Benutzer von der Passwortänderung in Kenntnis zu setzen.



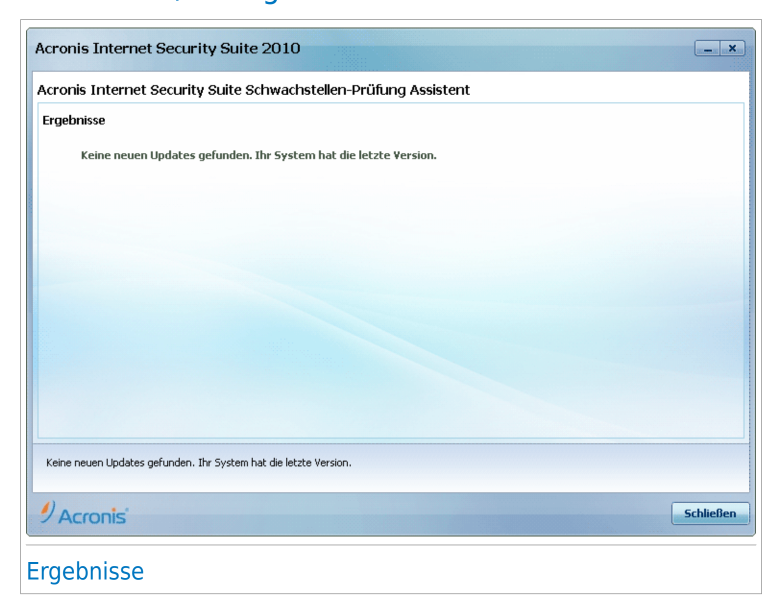
Anmerkung

Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (so wie #, $ or @). Sie können sich Online informieren um ein sicheres Passwort zu erstellen.

Klicken Sie auf **OK**, um das Passwort zu ändern.

Klicken Sie auf **Weiter**.

10.3.6. Schritt 6/6 - Ergebnisse betrachten



Ergebnisse

Klicken Sie auf **Schließen**.

10.4. Datentresor Assistent

Der Datentresorassistent hilft Ihnen beim Erstellen und Verwalten der Acronis Internet Security Suite 2010 Datentresore. Ein Datentresor ist ein verschlüsselter Speicherplatz auf Ihrem PC in welchem wichtige Daten sicher verstaut werden können, Dokumente sowie komplette Ordner.

Diese Assistenten erscheinen nicht, wenn Sie Probleme lösen, weil Datei-Datentresore eine optionale Methode zum Schutz Ihrer Daten sind. Sie können nur von Oberfläche des 'Intermediate-Modus' von Acronis Internet Security Suite 2010 heraus gestartet werden, von der Registerlasche **Dateispeicher** – und zwar wie folgt:

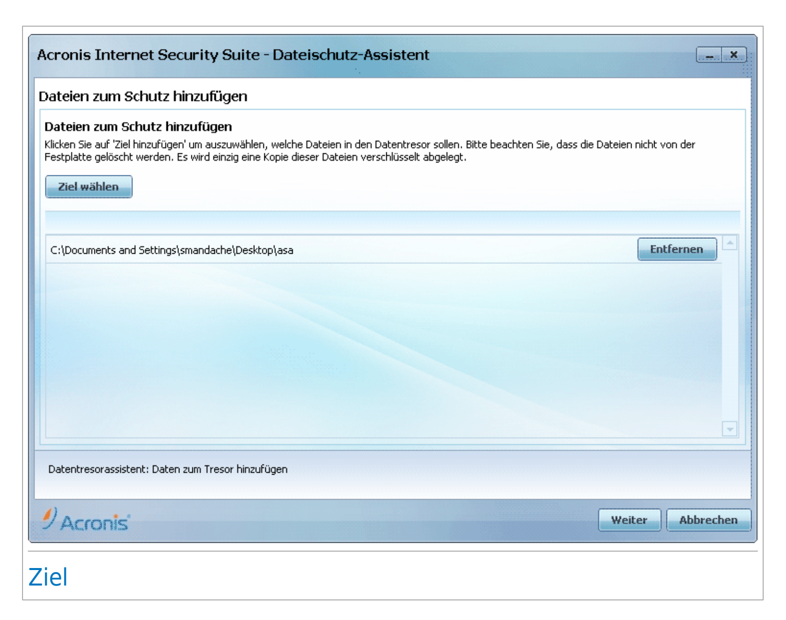
- **Datei zum Schutz hinzufügen** - Startet den Assistenten zum Speichern Ihrer wichtigen Dateien/Dokumente in verschlüsselten Schutzlaufwerken.
- **Dateien aus dem Schutz entfernen** - Startet den Assistenten zum Löschen von Daten im Dateischutz.
- **Datentresor ansehen** - Startet den Assistenten mit dem Sie den Inhalt eines Dateischutzes einsehen können.
- **Datentresor verschließen** - Startet den Assistenten mit welchem Sie einen offenen Dateitresor verschließen, um dessen Inhalt zu schützen.

10.4.1. Dateien zum Schutz hinzufügen

Dieser Assistent hilft Ihnen einen Datentresor zu erstellen und ihm Daten hinzuzufügen um diese sicher auf Ihrem PC zu speichern.

Schritt 1/6 - Ziel wählen

Hier können Sie auswählen welche Dateien und Ordner zum Schutz hinzugefügt werden sollen.



Ziel

Klicken Sie auf **Ziel hinzufügen**, wählen Sie dann die Dateien und Ordner die hinzugefügt werden sollen und wählen Sie **OK**. Der Pfad der ausgewählten Position wird in der Spalte **Pfad** angezeigt. Wenn Sie die ausgewählte Position ändern möchten, klicken Sie einfach auf die nebenstehende Schaltfläche **Entfernen**.

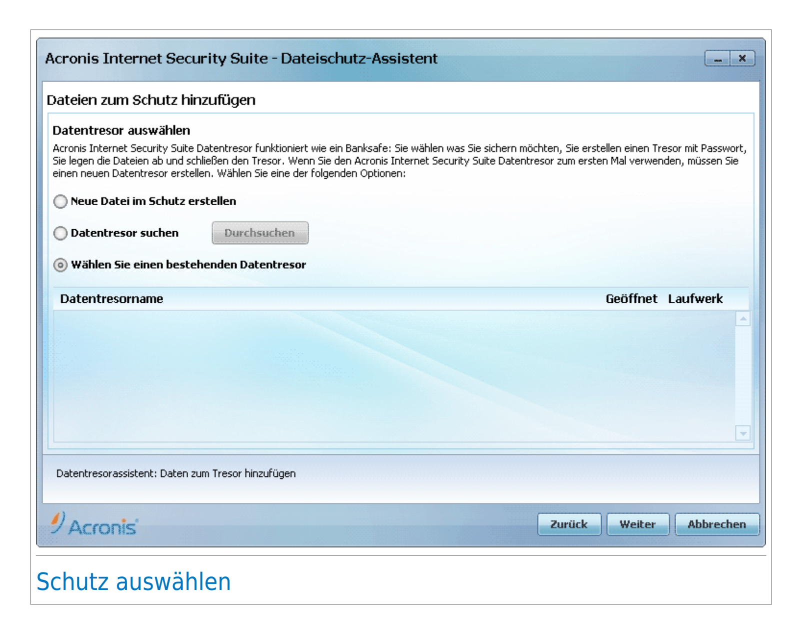


Anmerkung
Sie können eine oder auch mehrere Ziele auswählen.

Klicken Sie auf **Weiter**.

Schritt 2/6 - Schutz auswählen

Hier können Sie einen neuen Schutz erstellen oder einen existierenden auswählen.



Schutz auswählen

Wenn Sie **Nach Dateischutz suchen** auswählen, müssen Sie auf **Durchsuchen** klicken und den Dateischutz auswählen. Sie werden entweder zu Schritt 5 weitergeleitet, wenn der ausgewählte Schutz geöffnet ist (mounted) oder zu Schritt 4 wir wenn er verschlossen ist (unmounted).

Wenn Sie **Einen bestehenden Dateischutz wählen** auswählen, müssen Sie auf den gewünschten Schutznamen klicken. Sie werden entweder zu Schritt 5 weitergeleitet, wenn der ausgewählte Schutz geöffnet ist (mounted) oder zu Schritt 4 wir wenn er verschlossen ist (unmounted).

Wählen Sie **Neuen Dateischutz erstellen** wenn kein bestehender Schutz Ihren Bedürfnissen entspricht. Sie werden zu Schritt 3 weitergeleitet.

Klicken Sie auf **Weiter**.

Schritt 3/6 – Dateischutz erstellen

Hier können Sie genaue Informationen für den neuen Dateischutz angeben.



Schutz erstellen

Um die Informationen bezüglich des Dateischutzes anzugeben, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **Durchsuchen** und wählen Sie einen Ort für die bvd Datei.



Anmerkung
Bedenken Sie dass der Dateischutz eine verschlüsselte Datei auf Ihrem Computer mit der Endung bvd ist.

2. Wählen Sie einen Laufwerkbuchstaben für den neuen Dateischutz aus dem entsprechenden Menü.



Anmerkung
Bedenken Sie, dass beim Mounten der bvd Datei eine neue logische Partition (ein neues Laufwerk) erscheinen wird.

3. Geben Sie ein Passwort für den Dateischutz in das dafür vorgesehene Feld ein.



Anmerkung
Ihr Passwort muss mindestens 8 Zeichen lang sein.

4. Geben Sie das Passwort erneut ein.
5. Legen Sie die Größe des Dateischutzes fest (in MB), indem Sie den entsprechenden Wert in das dazugehörige Eingabefeld eintragen.

Klicken Sie auf **Weiter**.

Sie werden zu Schritt 5 weitergeleitet.

Schritt 4/6 - Passwort

Hier werden Sie nach der Eingabe des Passwortes für den ausgewählten Dateischutz gefragt.



Passwort eingeben

Geben Sie das Passwort in das entsprechende Feld ein und klicken Sie auf **Weiter**.

Schritt 5/6 - Zusammenfassung

Hier können Sie die gewählten Prozesse noch einmal betrachten.

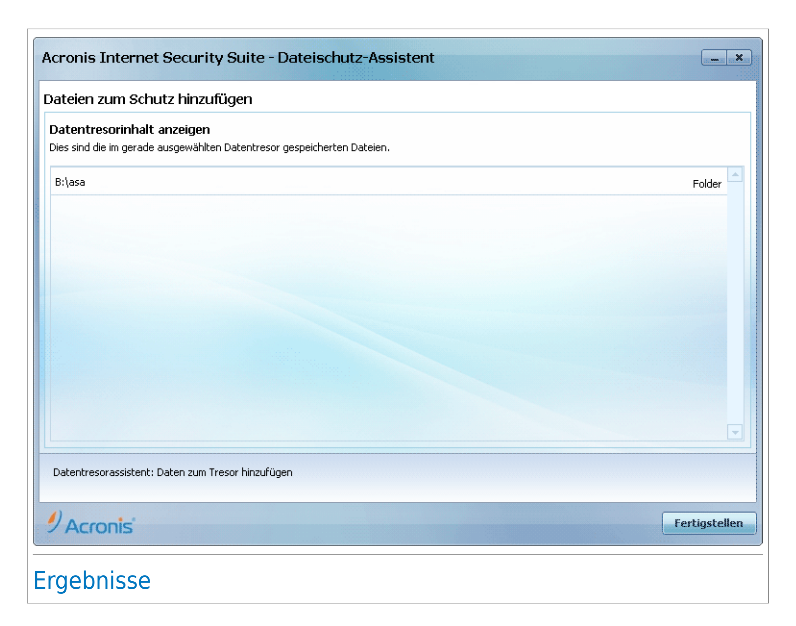


Übersicht

Klicken Sie auf **Weiter**.

Schritt 6/6 - Ergebnisse

Hier können Sie den Inhalt des Schutzes betrachten.



Ergebnisse

Klicken Sie auf **Fertigstellen**.

10.4.2. Dateien entfernen

Dieser Assistent hilft Ihnen Daten aus einem bestimmten Datentresor zu entfernen.

Schritt 1/5 - Schutz wählen

Hier können Sie den Schutz auswählen, aus dem die Dateien entfernt werden sollen.



Schutz auswählen

Wenn Sie **Nach einem Dateischutz suchen** auswählen, müssen Sie auf **Durchsuchen** klicken und den Dateischutz auswählen. Sie werden entweder zu Schritt 3 weitergeleitet wenn der Schutz geöffnet ist (mounted) oder zu Schritt 2 wenn er geschlossen ist (unmounted).

Wenn Sie auf **Einen bestehenden Dateischutz auswählen** klicken, müssen Sie auf den gewünschten Schutznamen klicken. Sie werden entweder zu Schritt 3 weitergeleitet wenn der Schutz geöffnet ist (mounted) oder zu Schritt 2 wenn er geschlossen ist (unmounted).

Klicken Sie auf **Weiter**.

Schritt 2/5 - Passwort

Hier werden Sie nach der Eingabe des Passwortes für den ausgewählten Dateischutz gefragt.



Passwort eingeben

Geben Sie das Passwort in das entsprechende Feld ein und klicken Sie auf **Weiter**.

Schritt 3/5 – Dateien auswählen

Hier erhalten Sie die Liste der Dateien des zuvor ausgewählten Schutzes.



Dateien auswählen

Wählen Sie die Dateien die entfernt werden sollen und klicken Sie auf **Weiter**.

Schritt 4/5 - Zusammenfassung

Hier können Sie die gewählten Prozesse noch einmal betrachten.



Übersicht

Klicken Sie auf **Weiter**.

Schritt 5/5 - Ergebnisse

Hier können Sie das Ergebnis der Operation sehen.



Ergebnisse

Klicken Sie auf **Fertigstellen**.

10.4.3. Datentresor öffnen

Dieser Assistent hilft Ihnen einen spezifischen Datentresor zu öffnen und die beinhaltende Dateien zu sehen.

Schritt 1/4 - Schutz wählen

Hier können Sie auswählen von welchem Dateischutz die Dateien betrachtet werden sollen.



Schutz auswählen

Wenn Sie **Nach einem Dateischutz suchen** auswählen, müssen Sie auf **Durchsuchen** klicken und den Dateischutz auswählen. Sie werden entweder zu Schritt 3 weitergeleitet wenn der Schutz geöffnet ist (mounted) oder zu Schritt 2 wenn er geschlossen ist (unmounted).

Wenn Sie auf **Einen bestehenden Dateischutz auswählen** klicken, müssen Sie auf den gewünschten Schutznamen klicken. Sie werden entweder zu Schritt 3 weitergeleitet wenn der Schutz geöffnet ist (mounted) oder zu Schritt 2 wenn er geschlossen ist (unmounted).

Klicken Sie auf **Weiter**.

Schritt 2/4 - Passwort

Hier werden Sie nach der Eingabe des Passwortes für den ausgewählten Dateischutz gefragt.



Passwort eingeben

Geben Sie das Passwort in das entsprechende Feld ein und klicken Sie auf **Weiter**.

Schritt 3/4 - Zusammenfassung

Hier können Sie die gewählten Prozesse noch einmal betrachten.



Übersicht

Klicken Sie auf **Weiter**.

Schritt 4/4 - Ergebnisse

Hier können Sie die Dateien des Schutzes sehen.



Ergebnisse

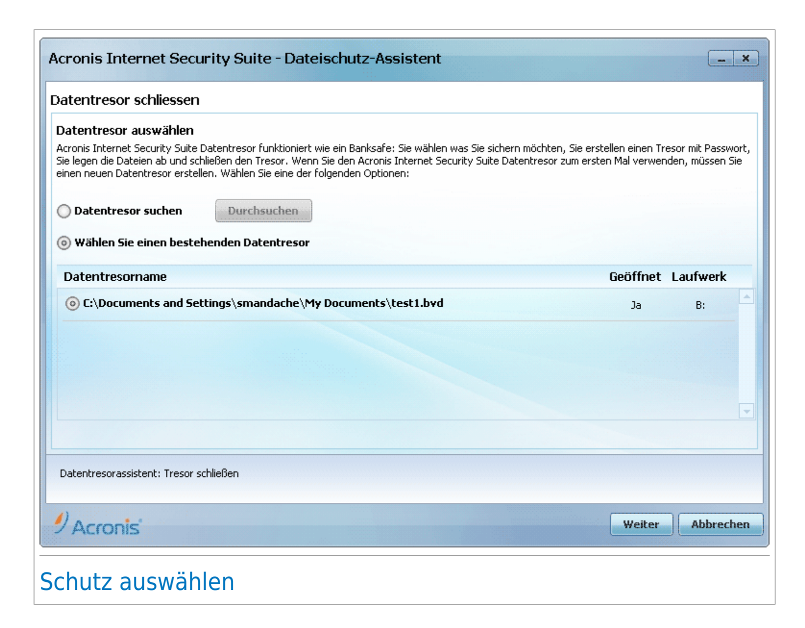
Klicken Sie auf **Fertigstellen**.

10.4.4. Datentresor schliessen

Dieser Assistent hilft Ihnen einen bestimmten Datentresor zu verschliessen um dessen Inhalt zu sichern.

Schritt 1/3 - Schutz wählen

Hier können Sie den Schutz auswählen der abgeschlossen werden soll.



Schutz auswählen

Wenn Sie **Nach einem Dateischutz suchen** auswählen müssen Sie auf **Durchsuchen** klicken und den Dateischutz auswählen.

Wenn Sie auf**Einen bestehenden Dateischutz wählen** klicken, dann müssen Sie den gewünschten Schutznamen anklicken.

Klicken Sie auf **Weiter**.

Schritt 2/3 - Zusammenfassung

Hier können Sie die gewählten Prozesse noch einmal betrachten.

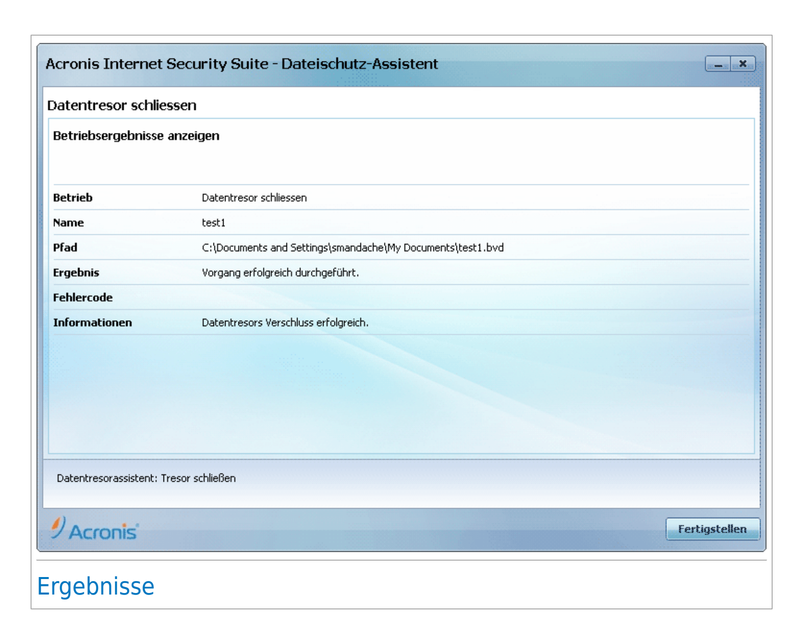


Übersicht

Klicken Sie auf **Weiter**.

Schritt 3/3 - Ergebnisse

Hier können Sie das Ergebnis der Operation sehen.



Ergebnisse

Klicken Sie auf **Fertigstellen**.

Standard-Ansicht

11. Dashboard

Das Dashboard liefert Informationen zum Sicherheitsstatus Ihres PC's und erlaubt es Ihnen ausstehende Risiken zu beheben.



Dashboard

Das Dashboard besteht aus folgenden Bereichen:

- **Allgemeiner Status** Zeigt Ihnen die Anzahl der Risiken die Ihrem Rechner gefährden und hilft Ihnen diese zu beheben. Wenn es noch offene Risiken gibt so werden Sie einen **roten Kreis mit einem Ausrufezeichen** sehen, und die **Alle Risiken beheben**-Schaltfläche. Klicken Sie auf die Schaltfläche um zum Problembehebnungsassistenten zu gelangen.
- **Status Detail** - zeigt den Status jedes Hauptmoduls, unter Verwendung eindeutiger Sätze und eines der folgenden Symbole:

  Grüner Kreis mit einem Häkchen: Keine Risiken beeinflussen den Sicherheitsstatus. Ihr Rechner und Ihre Daten sind geschützt.

  Grauer Kreis mit einem Ausrufezeichen: Die Aktivität dieser Modulkomponenten wird nicht überwacht. Daher liegen keine Informationen zum Sicherheitsstatus vor. Es könnten möglicherweise, spezifische Probleme mit diesen Modul existieren.

- **Roter Kreis mit einem Ausrufezeichen:** Risiken beeinflussen die Sicherheit Ihres Systems. Kritische Risiken erfordern Ihre unmittelbare Aufmerksamkeit. Nicht-kritische Risiken sollte auch alsbald Beachtung zukommen.

Klicken Sie auf den Namen eines Moduls um Einzelheiten zum Status zu erhalten und die Status Warnungen für diese Komponente zu konfigurieren.

- **Benutzer Profile** - Zeigt das momentane Benutzer Profil an und bietet einen Link zu einer relevanten Aufgabe für das Profil.

  - Wenn das **Standard** Profil ausgewählt ist, erlaubt Ihnen die **Jetzt Prüfen** Schaltfläche eine Systemprüfung unter Verwendung des Antivirus Prüfassistenten durchführen. Das gesamte System wird geprüft, außer Archive. In der standard Konfiguration wird nach allen Arten von Malware gesucht, außer nach rootkits.

  - Wenn das **Kindersicherungs**-Profil ausgewählt ist, lässt Sie die **Kindersicherungs**-Schaltfläche die Einstellungen konfigurieren. Für weitere Informationen zum konfigurieren der Kindersicherung lesen Sie bitte „*Kindersicherung*“ (S. 173).

  - Wenn der **Spiele** Modus ausgewählt ist, erlaubt die **Spiele Modus Ein/Aus schalten** Schaltfläche das Aktivieren/Deaktivieren des Spiele Modus. Der Spiele-Modus ändert die Schutzeinstellungen zeitweise, dass ihr Einfluss auf die Leistungsfähigkeit des Systems so gering wie möglich ist.

  - Wenn das **Benutzerdefiniert**-Profil ausgewählt ist, startet die **Jetzt Aktualisieren**-Schaltfläche unmittelbar das Update. Ein neues Fenster wird erscheinen, in dem Sie Status des Updates sehen können.

Wenn Sie in ein anderes Profil wechseln möchten oder das momentane Profil bearbeiten wollen, klicken Sie das auf das Profil und folgen dem Link Konifgurationsassistent.

12. Sicherheit

Acronis Internet Security Suite 2010 beinhaltet ein Sicherheitsmodul welches Ihr System virenfrei und Ihren Acronis Internet Security Suite 2010 auf dem neusten Stand hält. Um die verfügbaren Aktionen anzuzeigen klicken Sie auf den Reiter **Sicherheit**



Sicherheit

Das Sicherheitsmodul besteht aus zwei Bereichen:

- **Status Bereich** Zeigt Ihnen den aktuellen Status der wichtigsten überwachten Aufgaben und erlaubt Ihnen zu wählen, welche überwacht werden.
- **Schnellmaßnahmen** - Hier finden Sie die wichtigsten Sicherheitsaufgaben: jetzt Aktualisieren, Systemprüfung, Dokumentenprüfung, tiefgehende Systemprüfung, benutzerdefinierte Prüfung, Schwachstellenprüfung.

12.1. Statusbereich

Im Status Bereich können Sie die vollständige Liste der überwachten Sicherheitskomponenten und deren aktuellen Status sehen. Durch die Überwachung jedes Sicherheitsmoduls wird Acronis Internet Security Suite 2010 Sie nicht nur darüber informieren wenn Sie Einstellungen anpassen die die Sicherheit des Systems gefährden, sondern auch wenn wichtige Aufgaben vergessen wurden.

Der aktuelle Status einer Komponente wird angezeigt unter Verwendung eindeutiger Sätze und eines der folgenden Symbole:

Grüner Kreis mit einem Häkchen: Keine Risiken gefährden Ihren Computer.

Roter Kreis mit einem Ausrufezeichen: Risiken gefährden Ihren Computer.

Meinungen zum Problem sind in Rot aufgelistet. Klicken Sie auf **Beheben** um das jeweilige Problem zu beheben. Sollte ein Problem nicht direkt behoben werden, dann folgen Sie den Assistent.

12.1.1. Status-Warnmeldungen konfigurieren

Um die durch Acronis Internet Security Suite 2010 zu überwachenden Komponenten auszuwählen klicken Sie **Konfiguriere Status Warnungen** und wählen **Warnungen aktivieren** für die entsprechenden aus Optionen aus.



Wichtig

Wenn Sie über Risiken die die Sicherheit einer Komponente gefährden benachrichtigt werden möchten, so muss die Status Warnungen dieser aktiviert werden. Um zu gewährleisten, dass Ihr System komplett gesichert ist, aktivieren Sie bitte das Tracking für alle Komponenten und alle gemeldeten Probleme reparieren

Der Status folgender Sicherheitskomponente kann von Acronis Internet Security Suite 2010 verfolgt werden:

- **Antivirus** - Acronis Internet Security Suite 2010 beobachtet den Status der beiden Antivirus Komponenten: Echtzeitschutz und On-Demand Prüfung. Die häufigen Probleme, die für diesen Bestandteil berichtet wurden, werden in der folgenden Tabelle aufgelistet.

Risiko	Beschreibung
Echtzeitschutz ist deaktiviert	Alle Dateien werden bei Zugriff, durch Sie oder durch ein Programm auf dem System, nicht geprüft.
Sie haben Ihren Computer nie auf Maleware geprüft	Es wurde noch nie eine On-Demand Systemprüfung durchgeführt die sicherstellt dass die auf Ihrem PC gespeicherten Dateien Malware-frei sind.
Die letzte Systemprüfung die Sie gestartet haben wurde angehalten bevor dieser beendet wurde	Eine komplette Systemprüfung wurde gestartet aber nicht vervollständigt.
Antivirus befindet sich in einem kritischen Zustand	Echtzeitvirenschutz ist deaktiviert somit ist eine Systemprüfung überfällig.

- **Update** - Acronis Internet Security Suite 2010 überwacht das die Malware Signaturen aktuell sind. Die häufigen Probleme, die für diesen Bestandteil berichtet wurden, werden in der folgenden Tabelle aufgelistet.

Risiko	Beschreibung
Automatisches Update ist deaktiviert	Die Malware Signaturen Ihres Acronis Internet Security Suite 2010 Produktes werden nicht regelmäßig aktualisiert.
Das Update wurde seit x Tagen nicht durchgeführt	Ihre Acronis Internet Security Suite 2010 Malware-Signaturen sind nicht aktuell.

- **Firewall** - Acronis Internet Security Suite 2010 überwacht den Zustand der Firewall und ihrer Funktionen. Ist die Fireall nicht aktiv wird die Warnung **Firewall inaktiv** angezeigt.
- **Antispam** - Acronis Internet Security Suite 2010 überwacht den Status der Antispam-Funktion. Wenn diese nicht aktiviert ist, wird das Risiko **Antispam ist deaktiviert** angezeigt werden.
- **Antiphishing** - Acronis Internet Security Suite 2010 überwacht den Antiphishingstatus. Wenn es nicht für alle unterstützte Anwendungen aktiviert ist, wird die Meldung **Antiphishing ist deaktiviert** angezeigt.
- **Schwachstellen Prüfung** - Acronis Internet Security Suite 2010 überwacht die Schwachstellen Prüfung Komponente. Die Schwachstellen Prüfung informiert Sie über notwendige Windows Aktualisierungen, Anwendungs Aktualisierungen oder wenn ob Ihre Passwörter zu schwach sind.

  Die häufigen Probleme, die für diesen Bestandteil berichtet wurden, werden in der folgenden Tabelle aufgelistet.

Status	Beschreibung
Schwachstellenprüfung ist deaktiviert	Acronis Internet Security Suite 2010 prüft nicht nach potentiellen Schwachstellen in Bezug auf fehlende Windows/Anwendungs Aktualisierungen oder schwachen Passwörtern.
Mehrere Schwachstellen wurden entdeckt	Acronis Internet Security Suite 2010 hat fehlende Windows/Anwendungen Updates und/oder schwaches Passwort gefunden.
Wichtige Microsoft Updates	Kritische Microsoft Updates sind verfügbar, wurden aber nicht installiert.

Status	Beschreibung
Andere Microsoft Updates	Nicht-Kritische Microsoft Updates sind verfügbar, wurden aber nicht installiert.
Automatische Updates für Windows sind deaktiviert	Windows Sicherheitupdates werden, sobald diese verfügbar sind, nicht automatisch installiert.
Anwendungen (nicht Aktuell)	Eine neue Version der Anwendungist verfügbar, aber nicht installiert.
Benutzer (schwaches Passwort)	Ein Benutzerpassword kann von böswilligen Personen mit speziellen Programme herausgefunden werden.

12.2. Schnellmaßnahmen

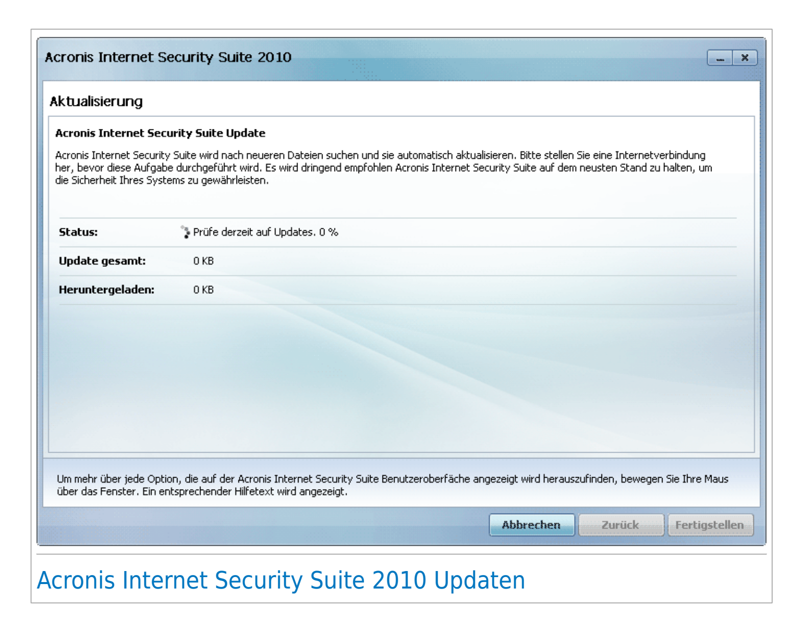
Hier finden Sie Links zu den wichtigsten Sicherheitsaufgaben:

- **Jetzt Aktualisieren** - startet ein sofortiges Update.
- **Systemprüfung** - startet eine standard Prüfung Ihres Systems (exklusive Archive). Für weitere On-Demand Prüfaufgaben, klicken Sie die Schaltfläche und wählen eine andere Prüfaufgabe: Meine Dokumente- oder tiefgehende Systemprüfung.
- **Benutzerdefinierte Prüfung** - startet einen Assistenten, mit dem Sie eine individuelle Prüfung erstellen und starten können.
- **Schwachstellenprüfung** - startet einen Assistenten der Ihnen beim Finden und Beheben von Schwachstellen in Ihrem System behilflich ist.

12.2.1. Acronis Internet Security Suite 2010 Updaten

Jeden Tag werden neue Viren entdeckt und identifiziert. Aus diesem Grund ist es von großer Bedeutung, dass Sie das Programm Acronis Internet Security Suite 2010 stets mit den neuesten Virensignaturen betreiben.

In der Standardeinstellung sucht Acronis Internet Security Suite 2010 nach Updates wenn Sie Ihren Computer einschalten und dann **jede weitere Stunde** erneut. Wenn Sie Acronis Internet Security Suite 2010 selbst aktualisieren möchten, klicken Sie auf **Jetzt aktualisieren**. Der Update-Prozess wird gestartet und das folgende Fenster wird erscheinen:



Acronis Internet Security Suite 2010 Updaten

In diesem Fenster können Sie den Status des Update-Prozesses sehen.

Der Updatevorgang wird "on the fly" durchgeführt, das bedeutet, dass die entsprechenden Dateien stufenweise aktualisiert werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System wird nicht gefährdet.

Wenn Sie dieses Fenster schließen möchten, klicken Sie einfach auf **Abbrechen**. Dies wird den Update-Prozess nicht anhalten.



Anmerkung

Falls Sie über eine Internetverbindung per Einwahl verfügen, ist es sinnvoll, regelmäßig ein manuelles Acronis Internet Security Suite 2010-Update durchzuführen.

Bitte starten Sie Ihren Computer neu, wenn dies verlangt wird. Im Falle von wichtigen Updates, werden Sie aufgefordert, Ihren Computer neu zu starten. Klicken Sie auf **Neustart** um Ihr System unverzüglich neuzustarten.

Wenn Sie Ihr System später neustarten möchten, klicken Sie auf **OK**. Wir empfehlen Ihnen, das System so schnell wie möglich neuzustarten.

12.2.2. Prüfen mit Acronis Internet Security Suite 2010

Um Ihren Computer auf Malware zu prüfen, führen Sie eine Scan-Aufgabe durch, indem Sie auf die entsprechende Schaltfläche klicken. Die folgende Tabelle zeigt Ihnen die verfügbaren San-Aufgaben mit einer Kurzbeschreibung:

Aufgabe	Beschreibung
Systemprüfung	Prüft alle Dateien mit Ausnahme von Archiven. In der standard Konfiguration, wird nach allen Arten von Malware geprüft, ausser rootkits.
Meine Dokumente prüfen	Verwenden Sie diese Aufgabe, um wichtige Ordner zu prüfen: `Meine Dokumente`, `Desktop` und `Autostart`. Das gewährleistet die Sicherheit Ihrer Dokumente, einen sicheren Arbeitsbereich und saubere Anwendungen die beim Start ausgeführt werden.
Tiefgehende Systemprüfung	Prüft das komplette System In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Prüfung anpassen	Verwenden Sie diese Aufgabe um spezielle Dateien und Ordner zu wählen, die geprüft werden sollen.



Anmerkung

Da die Prüfvorgänge **Tiefgehende Systemprüfung** und **Systemprüfung** das gesamte System prüfen kann der Vorgang einige Zeit dauern. Daher empfehlen wir Ihnen die Aufgabe mit niedriger Priotität durchzuführen oder wenn Sie das System nicht verwenden.

Wenn Sie eine Systemprüfung, Tiefgehende Systemprüfung oder Dokumentenprüfung durchführen, wird der Antivirus Prüfassistent erscheinen. Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen. Weitere Informationen zu diesem Assistenten finden Sie unter „*Antivirus Prüfassistent*" (S. 44).

Wenn Sie einen Benutzerdefinierte Prüfung durchführen, wird ein Assistent Sie durch den Prüfprozess begleiten. Folgen Sie den Sechsschritt angezeigte Verfahren, um spezifische Dateien oder Ordner zu prüfen. Weitere Informationen zu diesem Assistenten finden Sie unter „*Prüfassistent anpassen*" (S. 49).

12.2.3. Prüfung auf Schwachstellen/Anfälligkeit

Die Prüfung auf Schwachstellen überprüft die Microsoft Windows Updates, Microsoft Windows Office Updates und die Passwörter Ihrer Microsoft Windows Benutzerkonten, um sicherzustellen, dass Ihr Betriebssystem auf dem neusten Stand ist und keine Anfälligkeit für eine Passwortumgehung besteht.

Um Ihren Computer auf Schwachstellen zu prüfen, klicken Sie auf **Prüfung auf Schwachstellen** und folgen Sie den Schritten des Assistenten. Für weitere Informationen lesen Sie bitte „*Schwachstellen beheben*" (S. 233).

13. Kindersicherung

Acronis Internet Security Suite 2010 enthält ein Kindersicherungsmodul. Die Kindersicherung erlaubt es Ihnen den Zugriff Ihrer Kinder auf das Internet und für bestimmte Anwendungen einzuschränken. Um den Status der Kindersicherung zu prüfen, klicken Sie das **Kindersicherung** Tab.



Kindersicherung

Das Kindersicherungsmodul besteht aus zwei Bereichen:

- **Status Area** - Lässt Sie erkennen ob die Kindersicherung konfiguriert ist und das Überwachen der Modulaktivität aktiviert/deaktiviert.
- **Schnelle Aufgaben** - Hier finden Sie die wichtigsten Sicherheitsaufgaben: Systemprüfung, Tiefe Systemprüfung, jetzt aktualisieren.

13.1. Statusbereich

Der aktuelle Status der Kindersicherung wird angezeigt unter Verwendung eindeutiger Sätze und eines der folgenden Symbole:

Grüner Kreis mit einem Häkchen: Keine Risiken gefährden Ihren Computer.

Roter Kreis mit einem Ausrufezeichen: Risiken gefährden Ihren Computer.

Meinungen zum Problem sind in Rot aufgelistet. Klicken Sie auf **Beheben** um das jeweilige Problem zu beheben. Die häufigste Warnung, die für dieses Modul angezeigt wird ist **Kindersicherung nicht konfiguriert**.

Wenn Sie wollen, dass Acronis Internet Security Suite 2010 das Modul zur Kindersicherung überwacht, klicken Sie auf **Status-Warnmeldungen konfigurieren** und aktivieren Sie für dieses Modul das Kontrollkästchen **Warnungen aktivieren**.

13.2. Schnellmaßnahmen

Klicken Sie zur Konfiguration der Zugangssteuerung auf **Kindersicherung** im Quick Task-Bereich. Ein neues Fenster wird sich öffnen.



Kindersicherung konfigurieren.

Hier können sie den Status der Kindersicherung für jedes Windows Benutzerkonto sehen und die Kondersicherungsregeln konfigurieren. Dieses Konfigurationsfenster ist ähnlich zum Kindersicherungs-Tab in der erweiterten Ansicht. Für weitere Informationen lesen Sie bitte *„Kindersicherung“* (S. 173).

14. Datentresor

Acronis Internet Security Suite 2010 beinhaltet einen Datentresor Modul, der Ihnen dabei hilft Ihre Daten nicht nur sicher, sondern auch vertraulich aufzubewahren. Um dies durchzuführen, benutzen Sie die Dateiverschlüsselung.

Um in das Datentresor Modul zu gelangen, klicken Sie das **Datentresor)** Tab an.



Datentresor

Das Kindersicherungsmodul besteht aus zwei Bereichen:

- **Überwachte Komponenten** - Erlaubt es Ihnen die Liste aller überwachten Komponenten zu sehen. Sie können sich aussuchen welche der Komponenten überwacht werden sollen. Es ist empfohlen die Überwachungsfunktion für alle zu aktivieren.
- **Scnhellmaßnahmen** - Hier finden Sie die wichtigsten Sicherheitsaufgaben: Datentresore anlegen, anzeigen, sperren und entfernen.

14.1. Statusbereich

Der aktuelle Status einer Komponente wird angezeigt unter Verwendung eindeutiger Sätze und eines der folgenden Symbole:

Grüner Kreis mit einem Häkchen: Keine Risiken gefährden Ihren Computer.

Roter Kreis mit einem Ausrufezeichen: Risiken gefährden Ihren Computer.

Meinungen zum Problem sind in Rot aufgelistet. Klicken Sie auf **Beheben** um das jeweilige Problem zu beheben. Sollte ein Problem nicht direkt behoben werden, dann folgen Sie den Assistent.

Der Statusbereich im Datentresor-Tab bietet Informationen bezüglich Status des **Dateiverschlüsselungs** Moduls.

Wenn Sie wollen, daß Acronis Internet Security Suite 2010 die Dateiverschlüsselung überwacht, klicken Sie auf **Konfiguriere Status Warnungen** und wählen Sie **Warnungen aktivieren** für diesen Modul.

14.2. Schnellmaßnahmen

Folgende Aktionen stehen zur Verfügung:

- **Datei zum Schutz hinzufügen** - Startet den Assistenten zum Speichern Ihrer wichtigen Dateien/Dokumente in verschlüsselten Schutzlaufwerken. Weitere Informationen finden Sie unter *„Dateien zum Schutz hinzufügen“* (S. 63).
- **Dateien aus dem Schutz entfernen** - Startet den Assistenten zum Löschen von Daten im Dateischutz. Weitere Informationen finden Sie unter *„Dateien entfernen“* (S. 69).
- **Datentresor ansehen** - Startet den Assistenten mit dem Sie den Inhalt eines Dateischutzes einsehen können. Weitere Informationen finden Sie unter *„Datentresor öffnen“* (S. 74).
- **Datentresor verschließen** - Startet den Assistenten mit welchem Sie einen offenen Dateitresor verschließen, um dessen Inhalt zu schützen. Weitere Informationen finden Sie unter *„Datentresor schliessen“* (S. 78).

15. Netzwerk

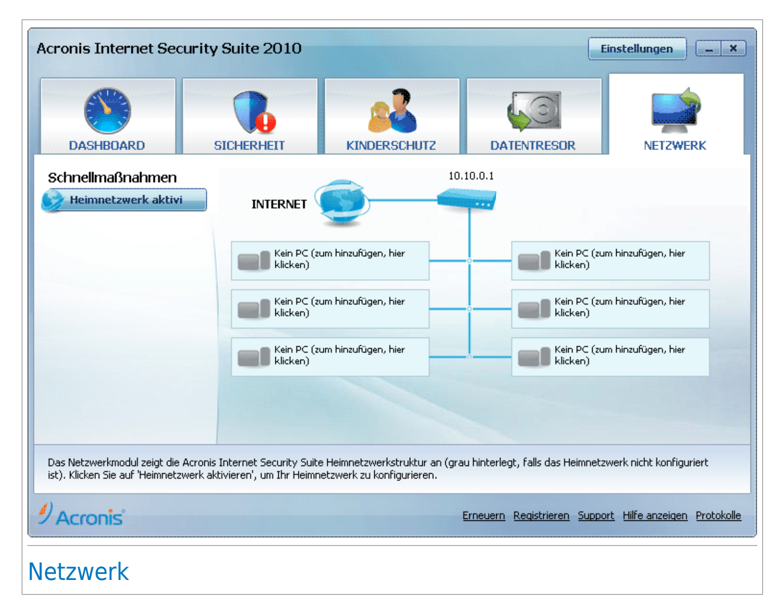
Mit dem Netzwerk-Modul können Sie die Acronis Produkte die auf den Computern in Ihrem Haushalt installiert sind von einem Computer aus verwalten. Um das Netzwerk-Modul einzurichten, klicken Sie das **Netzwerk**Tab.



Wichtig

Sie können nur die folgenden Acronis Sicherheitsprodukte verwalten:

- Acronis AntiVirus 2010
- Acronis Internet Security Suite 2010
- Acronis Backup and Security 2010



Netzwerk

Um die Acronis Produkte, die auf den Computern in Ihrem Haushalt installiert sind verwalten zu können, befolgen Sie diese Schritte:

1. Fügen Sie Ihren Computer dem Acronis Home-Netzwerk hinzu. Das Hinzufügen zu einem Netzwerk besteht aus dem Konfigurieren eines administrativen Passworts für die Verwaltung des Home-Netzwerks.
2. Fügen Sie jeden Computer, den Sie verwalten möchten dem Home-Netzwerk hinzu (Passwort einstellen).
3. Fügen Sie die Computer die Sie verwalten möchten ebenfalls auf Ihrem Computer hinzu.

15.1. Schnellmaßnahmen

Anfangs steht nur eine Schaltfläche zur Verfügung.

- **Netzwerk beitreten/erstellen** - bietet Ihnen die Möglichkeit ein Netzwerkpasswort einzustellen, um dem Netzwerk beizutreten.

Nach dem Beitreten zum Netzwerk werden mehrere Schaltflächen erscheinen.

- **Netzwerk verlassen** - bietet Ihnen die Möglichkeit das Netzwerk zu verlassen.
- **Computer hinzufügen** - erlaubt es Ihnen Computer dem Netzwerk hinzuzufügen.
- **Alle prüfen** - bietet Ihnen die Möglichkeit alle verwalteten Computer gleichzeitig zu prüfen.
- **Alle aktualisieren** - bietet Ihnen die Möglichkeit alle verwalteten Computer gleichzeitig zu aktualisieren.

15.1.1. Dem Acronis-Netzwerk beitreten

Um dem Acronis Home-Netzwerk beizutreten, befolgen Sie diese Schritte:

1. Klicken Sie **Netzwerk aktivieren**. Sie werden dazu aufgefordert, das Passwort für die Home-Verwaltung zu konfigurieren.



Passwort konfigurieren

2. Geben Sie das selbe Passwort in jedes der Editierfelder ein.
3. Klicken Sie auf **OK**.

Sie sehen den Namen des Computers in der Netzwerkübersicht.

15.1.2. Computer zum Acronis-Netzwerk hinzufügen

Um einen Computer zum Acronis Home-Netzwerk hinzuzufügen, müssen Sie zuerst das Passwort der Acronis Home-Verwaltung auf dem entsprechenden Computer konfigurieren.

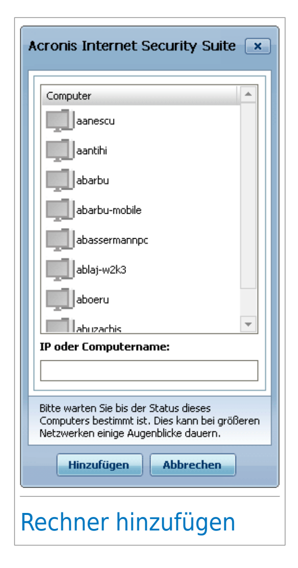
Um einen Computer zum Acronis Home-Netzwerk hinzuzufügen, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **PC hinzufügen**. Sie werden dazu aufgefordert, das Passwort für die lokale Home-Verwaltung anzugeben.



Passwort eingeben

2. Geben Sie das Passwort für die Home-Verwaltung ein und klicken Sie auf **OK**. Ein neues Fenster wird sich öffnen.



Rechner hinzufügen

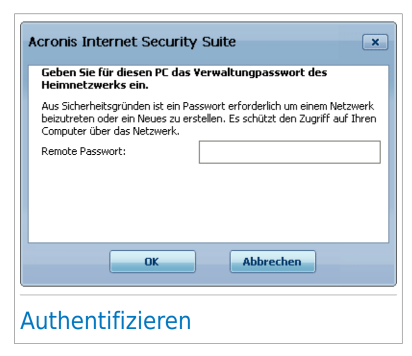
Sie können eine Liste der Computer im Netzwerk sehen. Die Bedeutung des Symbols ist wie folgt:

Verdeutlicht einen online befindlichen Computer, auf dem kein verwaltbares Acronis-Produkt installiert ist.

Verdeutlicht einen online befindlichen Computer, auf dem ein verwaltbares Acronis-Produkt installiert ist.

Verdeutlicht einen offline befindlichen Computer, auf dem ein verwaltbares Acronis-Produkt installiert ist.

3. Sie können hierzu eine der folgenden Methoden wählen:
   - Wählen Sie aus der Liste den Namen des Computers der hinzugefügt werden soll:
   - Geben Sie die IP-Adresse oder den Namen des Computers, der hinzugefügt werden soll in das dafür vorgesehene Feld ein.
4. Klicken Sie auf **Hinzufügen**. Sie werden dazu aufgefordert, das Passwort der Home-Verwaltung für den entsprechenden Computer einzugeben.



Authentifizieren

5. Geben Sie das Passwort für die Home-Verwaltung ein, das auf dem entsprechenden Computer konfiguriert wurde.
6. Klicken Sie auf **OK**. Wenn Sie das korrekt Passwort angegeben haben, wird der ausgewählte Computername in der Netzwerkübersicht erscheinen.



Anmerkung
Sie können bis zu fünf Computern zu der Netzwerkübersicht hinzufügen.

15.1.3. Das Acronis-Netzwerk verwalten

Wenn Sie das Acronis Home-Netzwerk erstellt haben, können Sie alle Acronis Produkte von einem Computer aus verwalten.



Netzwerkübersicht

Wenn Sie den Mauszeiger auf einen Computer der Netzwerkübersicht bewegen, können Sie einige Informationen über diesen sehen (Name, IP-Adresse, Anzahl der Probleme die die Systemsicherheit betreffen).

Wenn Sie mit der rechten Mautaste auf einen Computernamen im Netzwerk klicken, können Sie alle administrativen Aufgaben sehen, die Sie auf dem Remote-Computer ausführen können.

- **Aus diesem Netzwerk entfernen**

  Erlaubt Ihnen einen Pc aus dem Netzwerk entfernen.

- **Passwort für Einstellungen festlegen**

  Erlaubt Ihnen einen Passwort zu erstellen um den Zugang zu den Acronis Einstellungen auf diesem PC einschränken.

- **On-Demand Prüfaufgabe starten**

  Lässt sie eine On-Demand Prüfung auf dem Remote-PC durchführen. Sie können jede der folgenden Prüfungen tätigen: Meine Dokumente- System-, oder tiefgehende System-Prüfung.

- **Alle Probleme auf diesem PC beheben**

  Lässt Sie alle Risiken die die Sicherheit Ihres Systems gefährden beheben, indem Sie dem Alle Risiken beheben Assistenten folgen.

- **Historie anzeigen/Ereignisse**

Erlaubt den Zugriff auf das **Historie&Ereignisse** Modul des auf diesem PC installierten Acronis Produkts.

- **Jetzt aktualisieren**

  Initialisiert das Updateprozess für das Acronis Produkt das auf diesen Computer installiert ist.

- **Kindersicherung Einstellungen**

  Erlaubt es die Alterskategorie festzulegen welche vom Kindersicherungs-Webfilter auf diesem PC verwendet werden soll: Kind, Jugendlicher oder Erwachsener.

- **Diesen Computer als Update-Server für dieses Netzwerk festlegen**

  Erlaubt Ihnen diesen Rechner als Update-Server einzurichten, für alle Rechner aus dem Netzwerk, wo Acronis installiert ist. Unter Verwendung dieser Option, wird der Internetverkehr verringert, weil nur ein Rechner aus dem Netzwerk sich an das Internet anschließt um die Updates herunterzuladen.

Bevor Sie eine Aufgabe auf einem bestimmten Computer ausführen können, werden Sie dazu aufgefordert das Passwort der lokalen Home-Verwaltung anzugeben.



Passwort eingeben

Geben Sie das Passwort für die Home-Verwaltung ein und klicken Sie auf **OK**.



Anmerkung

Wenn Sie mehrere Aufgaben durchführen möchten, dann wählen Sie **In dieser Sitzung nicht nochmals fragen**. Wenn Sie diese Option wählen, werden Sie während der laufenden Sitzung nicht nochmals nach einem Passwort gefragt.

15.1.4. Alle Computer prüfen

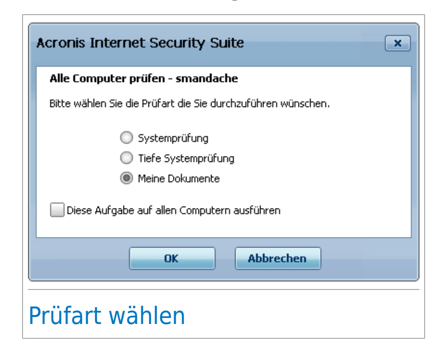
Um alle verwalteten Computer zu prüfen, befolgen Sie folgende Schritte:

1. Klicken Sie auf **Alle prüfen**. Sie werden dazu aufgefordert, das Passwort für die lokale Home-Verwaltung anzugeben.



Passwort eingeben

2. Wählen Sie eine Prüfart.
   - **Systemprüfung** - Prüft den gesamten Computer (ohne Archive).
   - **Tiefe Systemprüfung** - Führt einen Prüfvorgang für den gesamten Computer durch (einschließlich Archive).
   - **Meine Dokumente prüfen** - startet eine schnelle Prüfung Ihrer Dokumente und Einstellungen.



Prüfart wählen

3. Klicken Sie auf **OK**.

15.1.5. Alle Computer aktualisieren

Um alle verwalteten Computer zu aktualisieren, befolgen Sie folgende Schritte:

1. Klicken Sie auf**Alle aktualisieren** . Sie werden dazu aufgefordert, das Passwort für die lokale Home-Verwaltung anzugeben.



Passwort eingeben

2. Klicken Sie auf **OK**.

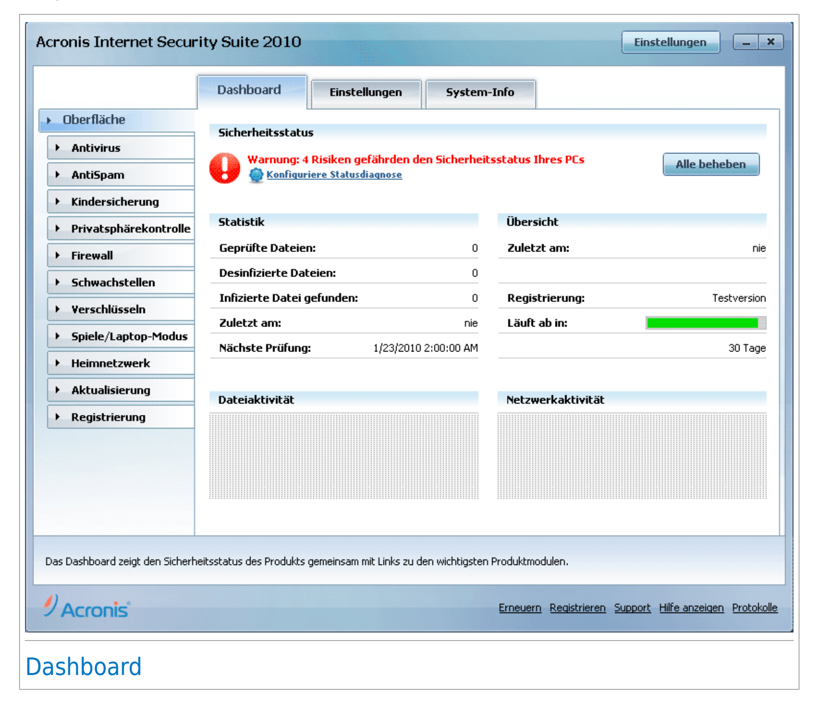
Profi Modus

16. Oberfläche

Das allgemeine Modul bietet Informationen über die Acronis Internet Security Suite 2010 Aktivität und das System. Hier können Sie auch das allgemeine Verhalten von Acronis Internet Security Suite 2010 ändern.

16.1. Dashboard

Um die Aktivitätsstatistiken des Produktes und Ihren Registrierungsstatus zu sehen, oder um zu sehen, ob Probleme Ihren Computer betreffen, gehen Sie zu **Allgemein>Dashboard** in der Profi-Ansicht.



Dashboard

Das Dashboard besteht aus mehreren Bereichen:

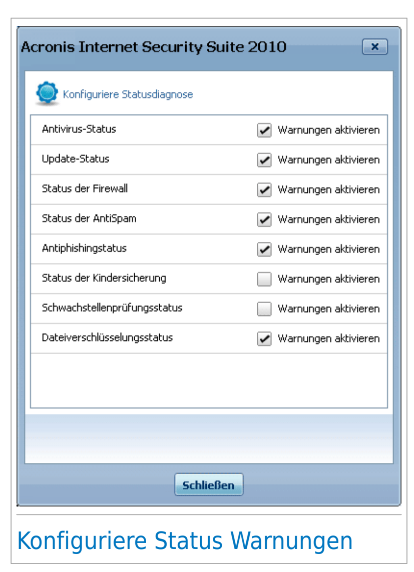
- **Allgemeiner Status** - Informiert Sie über die Risiken die Ihren Rechner gefährden.
- **Statistiken** - Zeigt wichtige Informationen bezüglich der Aktivität von Acronis Internet Security Suite 2010 an.
- **Overview** - Zeigt den Update Status, Registrierung und Lizenzinformationen.

- **Dateiaktivität** - Zeigt die Entwicklung der Anzahl der Objekte an, die von Acronis Internet Security Suite 2010 Antimalware geprüft wurden. Die Höhe der Leiste zeigt die Intensität des Datenverkehrs für diesen Zeitraum an.
- **Netzwerkaktivität** - Zeigt die Entwicklung des Netzwerk-Datenverkehrs an, der von der Acronis Internet Security Suite 2010 Firewall gefiltert wurde. Die Höhe der Leiste zeigt die Intensität des Datenverkehrs für diesen Zeitraum an.

16.1.1. Gesamt-Status

Hier können Sie die Anzahl der Risiken erkennen, die die Sicherheit ihres PC's betreffen. Um alle Bedrohungen zu entfernen, klicken Sie **Alle Risiken beheben**. Hierdurch wird der Alle Risiken beheben Assistent gestartet.

Um zu konfigurieren welche Module von Acronis Internet Security Suite 2010 überwacht werden, klicken Sie **Konfiguriere Status Warnungen**. Ein neues Fenster wird sich öffnen:



Konfiguriere Status Warnungen

Wenn Acronis Internet Security Suite 2010 eine Komponente überwachen soll, wählen Sie für diese Komponente die **Warnungen Aktivieren** Markierung. Der Status folgender Sicherheitskomponente kann von Acronis Internet Security Suite 2010 verfolgt werden:

- **Antivirus** - Acronis Internet Security Suite 2010 beobachtet den Status der beiden Antivirus Komponenten: Echtzeitschutz und On-Demand Prüfung. Die häufigen Probleme, die für diesen Bestandteil berichtet wurden, werden in der folgenden Tabelle aufgelistet.

Risiko	Beschreibung
Echtzeitschutz ist deaktiviert	Alle Dateien werden bei Zugriff, durch Sie oder durch ein Programm auf dem System, nicht geprüft.
Sie haben Ihren Computer nie auf Maleware geprüft	Es wurde noch nie eine On-Demand Systemprüfung durchgeführt die sicherstellt dass die auf Ihrem PC gespeicherten Dateien Malware-frei sind.
Die letzte Systemprüfung die Sie gestartet haben wurde angehalten bevor dieser beendet wurde	Eine komplette Systemprüfung wurde gestartet aber nicht vervollständigt.
Antivirus befindet sich in einem kritischen Zustand	Echtzeitvirenschutz ist deaktiviert somit ist eine Systemprüfung überfällig.

- **Update** - Acronis Internet Security Suite 2010 überwacht das die Malware Signaturen aktuell sind. Die häufigen Probleme, die für diesen Bestandteil berichtet wurden, werden in der folgenden Tabelle aufgelistet.

Risiko	Beschreibung
Automatisches Update ist deaktiviert	Die Malware Signaturen Ihres Acronis Internet Security Suite 2010 Produktes werden nicht regelmäßig aktualisiert.
Das Update wurde seit x Tagen nicht durchgeführt	Ihre Acronis Internet Security Suite 2010 Malware-Signaturen sind nicht aktuell.

- **Firewall** - Acronis Internet Security Suite 2010 überwacht den Zustand der Firewall und ihrer Funktionen. Ist die Fireall nicht aktiv wird die Warnung **Firewall inaktiv** angezeigt.
- **Antispam** - Acronis Internet Security Suite 2010 überwacht den Status der Antispam-Funktion. Wenn diese nicht aktiviert ist, wird das Risiko **Antispam ist deaktiviert** angezeigt werden.
- **Antiphishing** - Acronis Internet Security Suite 2010 überwacht den Antiphishingstatus. Wenn es nicht für alle unterstützte Anwendungen aktiviert ist, wird die Meldung **Antiphishing ist deaktiviert** angezeigt.
- **Kindersicherung** - Acronis Internet Security Suite 2010 überwacht den Zustand der Kindersicherung. Ist die Kindersicherung nicht aktiv wird die Warnung **Kindersicherung nicht konfiguriert** angezeigt.

- **Schwachstellen Prüfung** - Acronis Internet Security Suite 2010 überwacht die Schwachstellen Prüfung Komponente. Die Schwachstellen Prüfung informiert Sie über notwendige Windows Aktualisierungen, Anwendungs Aktualisierungen oder wenn ob Ihre Passwörter zu schwach sind.

  Die häufigen Probleme, die für diesen Bestandteil berichtet wurden, werden in der folgenden Tabelle aufgelistet.

Status	Beschreibung
Schwachstellenprüfung ist deaktiviert	Acronis Internet Security Suite 2010 prüft nicht nach potentiellen Schwachstellen in Bezug auf fehlende Windows/Anwendungs Aktualisierungen oder schwachen Passwörtern.
Mehrere Schwachstellen wurden entdeckt	Acronis Internet Security Suite 2010 hat fehlende Windows/Anwendungen Updates und/oder schwaches Passwort gefunden.
Wichtige Microsoft Updates	Kritische Microsoft Updates sind verfügbar, wurden aber nicht installiert.
Andere Microsoft Updates	Nicht-Kritische Microsoft Updates sind verfügbar, wurden aber nicht installiert.
Automatische Updates für Windows sind deaktiviert	Windows Sicherheitupdates werden, sobald diese verfügbar sind, nicht automatisch installiert.
Anwendungen (nicht Aktuell)	Eine neue Version der Anwendungist verfügbar, aber nicht installiert.
Benutzer (schwaches Passwort)	Ein Benutzerpassword kann von böswilligen Personen mit speziellen Programme herausgefunden werden.

- **Datei-Verschlüsselung** - BitDefender überwacht den Status des Datentresors. Wenn diese nicht aktiviert ist, wird die Warnung **Datenverschlüsselung deaktiviert** angezeigt.



Wichtig

Um zu gewährleisten, dass Ihr System komplett gesichert ist, aktivieren Sie bitte das Tracking für alle Komponenten und alle gemeldeten Probleme reparieren.

16.1.2. Statistik

Wenn Sie die Aktivität von Acronis Internet Security Suite 2010 überwachen möchten, können Sie das im Statistikbereich tun. Sie können folgende Objekte sehen:

Objekt	Beschreibung
Geprüfte Dateien	Zeigt die Anzahl der Dateien an, die während der letzten Prüfung auf Malware überprüft wurden.
Desinfizierte Dateien	Zeigt die Anzahl der Dateien an, die während der letzten Prüfung desinfiziert wurden.
Infizierte Dateien entdeckt	Zeigt die Anzahl der infizierten Dateien an, die während der letzten Prüfung gerfunden wurden.
Letzte Systemprüfung	Zeigt an wann Ihr Computer zu letzt geprüft worden ist. Wenn die letzte Prüfung länger als eine Woche her ist, führen Sie bitte so bald wie möglich eine solche durch. Um den gesamten Computer prüfen zu lassen, gehen Sie zu **Antivirus**, Virenprüfung Tab, und starten Sie entweder eine vollständige- oder tiefgehende Systemprüfung.
Nächste Prüfung	Zeigt an wann die nächste Systemprüfung Ihres PC's ansteht.

16.1.3. Übersicht

Hier können Sie den Updatestatus, Registrierungs- und Lizenz- informationen sehen.

Objekt	Beschreibung
Letztes Update	Zeigt an wann Ihr Acronis Internet Security Suite 2010 Produkt zu letzt aktualisiert worden ist. Bitte führen Sie regelmässige Updates durch um den vollen Schutz für Ihr System zu gewährleisten.
Registrierung	Zeigt Ihren Lizenzschlüssel und dessen Status an. Damit Ihr System sicher ist, müssen Sie Acronis Internet Security Suite 2010 erneuern oder aktualisieren, falls der Lizenzschlüssel abgelaufen ist.
Läuft ab in	Die Anzahl der Tage bis zum Ende des Lizenzschlüssels. Wenn Ihr Lizenzschlüssel innerhalb der nächsten Tage ablaufen sollte, registrieren Sie das Produkt bitte mit einem neuen Schlüssel. Um einen Lizenzschlüssel zu erwerben oder Ihre Lizenz zu erneuern, klicken Sie bitte den **Kaufen/Verlängern** Link, zu finden im unteren Teil des Fensters.

16.2. Einstellungen

Um allgemeine Einstellungen für Acronis Internet Security Suite 2010 vorzunehmen und zu verwalten klicken Sie auf **Allgemeine>Einstellungen** in der Profiansicht.



Allgemeine Einstellungen

Hier können Sie die umfassenden Einstellungen von Acronis Internet Security Suite 2010 einsehen. Standardmäßig wird Acronis Internet Security Suite 2010 beim Windowsstart geladen und läuft dann im Hintergrund.

16.2.1. Allgemeine Einstellungen

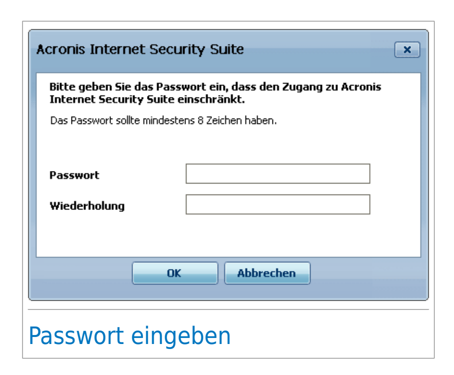
- **Passwortschutz für Programm-Einstellung aktivieren** - die Passwort-Einstellung aktivieren, um Ihre Acronis Internet Security Suite 2010-Einstellungen zu schützen.



Anmerkung

Wenn Sie nicht der einzige Benutzer des Computers mit administrativen Rechten sind, empfehlen wir Ihnen, Ihre vorgenommenen Einstellungen mit einem Passwort zu schützen.

Wenn Sie diese Option wählen erscheint das folgende Fenster:



Passwort eingeben

Schreiben Sie ein Passwort in das **Passwort**-Feld und wiederholen Sie es in dem Feld **Wiederholung**. Danach klicken Sie auf **OK**.

Wenn Sie das Passwort eingestellt haben, werden Sie immer danach gefragt, wenn Sie die Acronis Internet Security Suite 2010-Einstellungen ändern möchten. Ein anderer Systemadministrator (falls vorhanden) muss dieses Passwort ebenfalls angeben, um Acronis Internet Security Suite 2010-Einstellungen zu ändern.

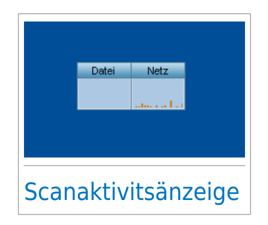
Wenn Sie nur während der Einstellung der Kindersicherung nach dem Passwort gefragt werden möchten, so aktivieren Sie auch **Passwort für Kindersicherung erfragen/anwenden**. Wenn ein Passwort nur für die Kindersicherung eingestellt wurde, und Sie diese Option nicht aktivieren, so wird das entsprechende Passwort bei der Einstellung jeder Acronis Internet Security Suite 2010-Option erfragt.



Wichtig

Falls Sie Ihr Passwort vergessen haben sollten, müssen Sie unter Reparieren Ihre Acronis Internet Security Suite 2010-Konfiguration modifizieren.

- **Bei Aktivierung der Kindersicherung fragen, ob ich das Passwort konfigurieren möchte** - wenn diese Option aktiviert ist und kein Passwort eingestellt wurde, werden Sie dazu aufgefordert ein Passwort einzustellen um die Kindersicherung zu aktivieren. Wenn Sie ein Passwort einstellen, können andere Benutzer mit administrativen Rechten die Einstellungen der Kindersicherung nicht verändern.
- **Acronis Internet Security Suite-News anzeigen** - von Zeit zu Zeit empfangen Sie Sicherheitsmeldungen, die von Acronis-Servern versendet werden.
- **Pop-Ups und Hinweise anzeigen** - Pop-up-Fenster anzeigen, die über den Produktstatus informieren. Sie können Acronis Internet Security Suite 2010 so konfigurieren das die Pop-ups angezeigt werden, wenn die Bedienoberfläche sich in Basis- / Standard- oder Profi-Modus befindet.
- **Aktivitsänzeige aktivieren (grafische Bildschirmanzeige der Produktaktivität)** - zeigt die Leiste der Scanaktivität an wenn Windows läuft. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie nicht möchten, dass die Scanaktivitätsleiste angezeigt wird.



Scanaktivitsänzeige



Anmerkung

Diese Option kann nur für das aktuelle Windows Benutzerkonto konfiguriert werden. Die Aktivitätsanzeige ist auschliesslich verfügbar wenn die Bedienoberfläche in der Profiansicht ist.

16.2.2. Virenbericht Einstellungen

- **Viren-Meldung an das Acronis Virus Labor** - sendet erkannte Viren an das Acronis-Virenlabor. Diese Meldung zeigt uns die Verbreitung von Viren an und hilft uns, geeignete Gegenmaßnahmen ergreifen zu können.

  Diese Meldungen beinhalten keine personifizierten Daten, wie Ihren Namen, IP-Adresse oder ähnliches. Diese werden nicht für kommerziele Zwecke verwendet. Die Meldungen beinhalten nur den Virennamen und werden für die Erstellung von Statistiken verwendet.

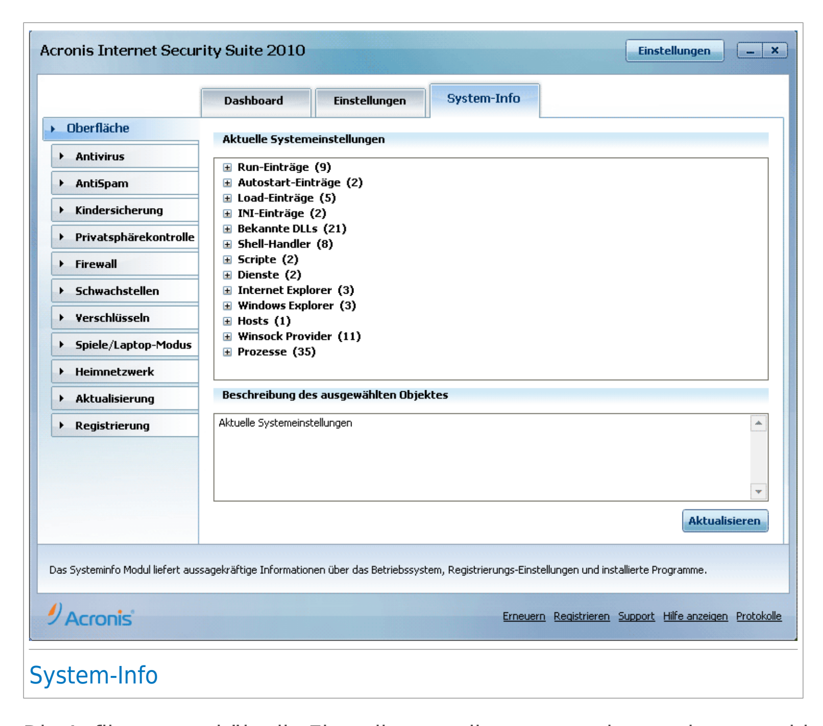
- **Aktiviere Acronis Internet Security Suite Outbreak-Erkennung** - sendet Berichte über potentiele Virenausbrüche an das Acronis Labor.

  Diese Meldungen beinhalten keine personifizierten Daten, wie Ihren Namen, IP-Adresse oder ähnliches. Diese werden nicht für kommerziele Zwecke verwendet. Die Meldungen beinhalten nur den Virennamen und werden nur für die Erkennung von neuen Viren verwendet.

16.3. System-Info

Acronis Internet Security Suite 2010 erlaubt Ihnen in einer einzigen Übersicht alle Einstellungen und Programme welche beim Systemstart gestartet werden einzusehen. Auf diese Weise können Sie die Aktivitäten des Systems und der darauf installierten Anwendungen, sowie mögliche Systeminfektionen überwachen.

Um diese Systeminformationen anzuzeigen klicken Sie auf **Allgemeine>System-Info** in der Profiansicht.



System-Info

Die Auflistung enthält alle Einstellungen die angewendet werden, sowohl wenn der Computer gestartet wird als auch wenn spezielle Anwendungen aufgerufen werden und gesonderte Regeln besitzen.

Drei Schaltflächen sind verfügbar:

- **Wiederherstellen** - stellt die ursprüngliche Dateiassoziation der aktuellen Datei wieder her. Nur für die Einstellungen **Dateiassoziationen** verfügbar!
- **Gehe zu** - öffnet ein Fenster mit der Pfadangabe für das Objekt (Zum Beispiel: **Eintragung**).



Anmerkung

Je nach ausgewähltem Objekt wird die Schaltfläche **Gehe zu** nicht erscheinen.

- **Aktualisieren** - öffnet erneut die das Menü **System-Info**.

17. Antivirus

Acronis Internet Security Suite 2010 schützt Sie vor allen Arten von Schädlingen (Virus, Trojaner, Spyware, Rootkits und so weiter). Der Virenschutz ist in zwei Kategorien aufgeteilt:

- Echtzeitschutz - hält neue Malware-Bedrohungen davon ab, in Ihr System zu gelangen. Acronis Internet Security Suite 2010 wird z.B. ein Worddokument auf Schädlinge prüfen wenn Sie es öffnen, und eine EMailnachricht wenn Sie diese empfangen.



Anmerkung

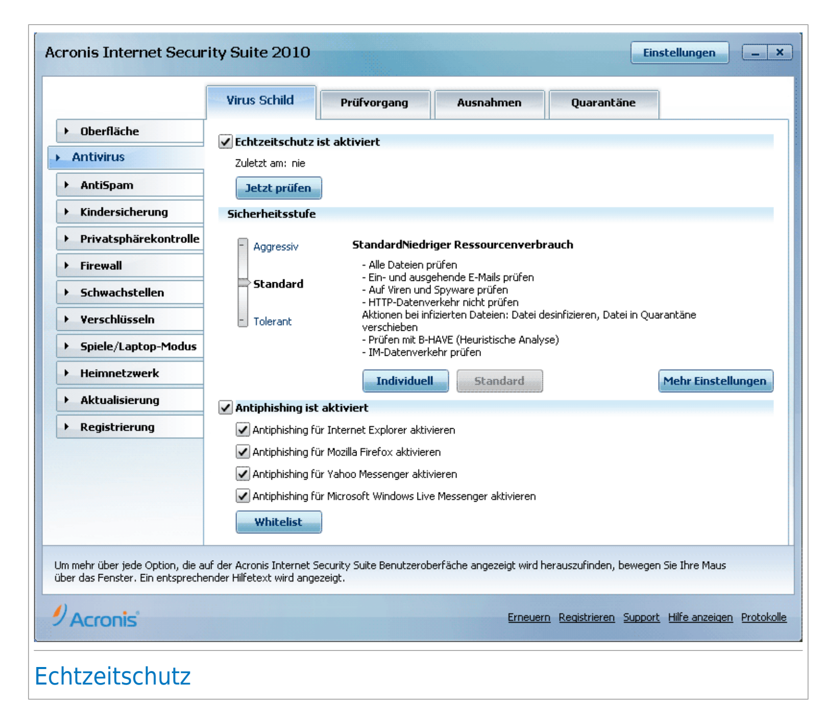
Der Echtzeitschutz gilt auch für die Prüfung auf Zugriff (On-Access) - Dateien werden geprüft, sobald die Benutzer auf sie zugreifen.

- On-demand Prüfung - erkennt und entfernt Malware die sich bereits auf dem System befindet. Hierbei handelt es sich um eine klassische , durch den Benutzer gestartete, Prüfung - Sie wählen das Laufwerk, Ordner oder Datei welche Acronis Internet Security Suite 2010 prüfen soll, und Acronis Internet Security Suite 2010 prüft diese. Die Prüfaufgaben erlauben Ihnen die Prüfroutinen auf Ihre Bedürfnisse anzupassen und diese zu einem festgelegten Zeitpunkt zu starten.

17.1. Echtzeitschutz

Acronis Internet Security Suite 2010 bietet einen dauerhaften Echtzeitschutz gegen verschiedene Malware, indem alle Dateien auf die zugegriffen wird sowie E-Mail-Nachrichten und die Kommunikationen per Instant Messaging Software (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) geprüft werden. Acronis Internet Security Suite 2010 Antiphishing gewährleistet einen sicheren Aufenthalt und den Schutz persönlicher Informationen im Internet. Der Benutzer wird über potentielle Phishing-Webseiten alarmiert.

Um den Echtzeitschutz und Antiphishingschutz zu konfigurieren klicken Sie auf **Antivirus>Schild** in der Profiansicht.



Echtzeitschutz

Sie können sehen ob der Echtzeitschutz aktiviert oder deaktiviert ist. Wenn Sie den Status des Echtzeitschutzes verändern möchten, markieren Sie das entsprechende Kontrollkästchen oder lassen Sie es frei.



Wichtig

Um zu verhindern, dass Viren Ihren Computer befallen, lassen Sie den **Echtzeitvirenschutz** immer aktiviert.

Um eine schnelle Systemprüfung durchzuführen klicken Sie auf **Jetzt prüfen**.

17.1.1. Sicherheitsstufe einstellen

Sie können die Sicherheitseinstellung an Ihre Anforderungen anpassen. Ziehen Sie die Anzeige auf der Scala auf die richtige Einstellung.

Es gibt 3 mögliche Einstellungen:

Sicherheitseinstellung	Beschreibung
Tolerant	Deckt einfache Anforderungen ab. Geringe Belastung der Ressourcen.

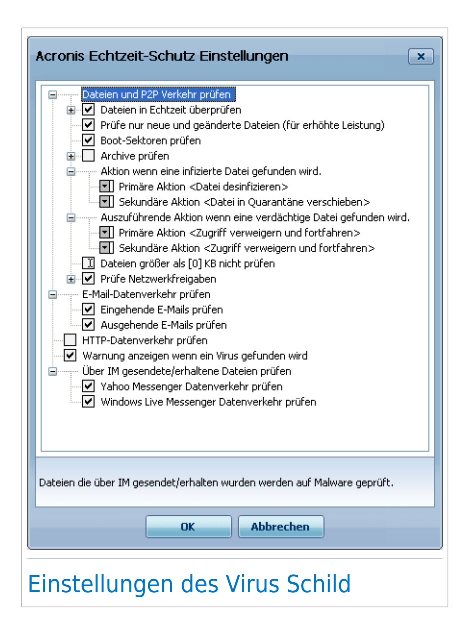
Sicherheitseinstellung	Beschreibung
	Nur Programme und eingehende Nachrichten werden auf Viren hin geprüft. Neben der klassischen Signaturen basierenden Prüfung wird außerdem die heuristische Prüfung eingesetzt. Bei infizierten Dateien können Sie wählen zwischen Datei bereinigen/in Quarantäne verschieben.
Standard	Gewährleistet Standard Sicherheit. Belastung der Ressourcen ist gering. Alle Dateien und eingehende&ausgehenden Nachrichten werden auf Viren und Spyware geprüft. Sowohl durch die klassische Prüfung wie auch der Heuristik. Bie infizierten Dateinen können Sie wählen zwischen Datei bereinigen/in Quarantäne verschieben.
Aggressiv	Gewährleistet hohe Sicherheit. Mittlere Belastung der Ressourcen. Alle Dateien und eingehende&ausgehenden Nachrichten und Web-Verkehr werden auf Viren und Spyware geprüft. Sowohl durch die klassische Prüfung wie auch der Heuristik. Bie infizierten Dateinen können Sie wählen zwischen Datei bereinigen/in Quarantäne verschieben.

Wenn Sie zu den Standardeinstellungen zurückkehren wollen, klicken Sie auf **Standard**.

17.1.2. Sicherheitsstufe anpassen

Benutzer mit Vorkenntnissen sollten sich die Prüfeinstellungen von Acronis Internet Security Suite 2010 genauer ansehen. Bestimmte Dateierweiterungen, Verzeichnisse und Archive, die wahrscheinlich keine Bedrohung darstellen, können vom Scan ausgeschlossen werden. So wird die Prüfzeit verringert und das Reaktionsvermögen Ihres Rechners während eines Scans verbessert.

Um die Echzeit-Sicherheitseinstellungen **anzupassen**, klicken Sie auf **Einstellung ändern**. Das folgende Fenster öffnet sich:



Einstellungen des Virus Schild

Die Prüfoptionen sind wie ein aufklappbares Windows-Explorermenü aufgebaut. Klicken Sie auf "+", um eine Option zu öffnen, und auf "-", um diese zu schließen.



Anmerkung

Sie können sehen, dass sich einige Prüfoptionen nicht öffnen lassen, obwohl das "+"-Zeichen sichtbar ist. Der Grund dafür ist, dass diese Optionen bisher nicht gewählt worden sind. Wenn Sie diese Optionen auswählen, können sie geöffnet werden.

- **Dateizugriffe und P2P-Übertragungen prüfen** - um alle Dateien und die Kommunikation mit Instant Messengers (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) zu überprüfen. Des Weiteren wählen Sie eine Datei aus, die Sie prüfen möchten.

Optionen		Beschreibung
Dateien prüfen	**Alle Dateien prüfen**	Alle Dateien, auf die zugegriffen wird, werden unabhängig von ihrem Typ geprüft.
	Nur Applikationen prüfen	Prüft ausschließlich Dateien mit den Dateiendungen: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`;

Optionen		Beschreibung
		.rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml und .nws.
	Nur Dateien mit folgenden Erweiterungen	Nur die Dateien werden überprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
	Auf Spyware prüfen	Risikosoftware erkennen. Erkannte Dateien werden als infiziert behandelt. Software welche diese Dateien verwendet könnte Ihre Arbeit einstellen falls diese Option aktiviert ist. Wählen Sie **Überspringe Dialer und Anwendungen bei der Prüfung** und/oder **Überspringe Keylogger bei der Prüfung** wenne Sie diese Art von Dateien von der Prüfung ausschliessen wollen.
Prüfe nur neue und geänderte Dateien		Prüfe nur Dateien welche zuvor nicht geprüft oder seit der letzten Prüfung geändert worden sind. Durch auswählen dieser Option verbessern Sie die allgemeine Systemreaktionsfähigkeit um ein vielfaches mit minimalen Sicherheitsabstrichen.
Boot-Sektoren		Prüft die Bootsektoren des Systems.
Archive prüfen		Auch der Inhalt von Archiven wird geprüft. Ist diese Option aktiviert, so kann es zur Verlangsamung des Computers führen. Sie können Die Maximalgrösse und die maximale Archivtiefe der zu prüfenden Archive einstellen (in Kilobytes, bei 0 werden alle geprüft).
Direktverbindung		Nun können Sie eine der folgenden Möglichkeiten auswählen:
	Zugriff verweigern und fortfahren	Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.
	Dateien desinfizieren	Den Malware-Code aus den entdeckten infizierten Dateien entfernen.

Optionen		Beschreibung
	Datei löschen	Infizierte Dateien werden ohne Warnung sofort gelöscht.
	In Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Aktionsoptionen		Wählen Sie hier eine Aktion, die ausgeführt werden soll, wenn die erste Aktion fehlschlägt.
	Zugriff verweigern und fortfahren	Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.
	Datei löschen	Infizierte Dateien werden ohne Warnung sofort gelöscht.
	In Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Dateien größer als [x] KB nicht prüfen		Geben Sie die maximale Dateigröße an, bis zu der Dateien gescannt werden sollen. Wenn Sie "0" eingeben werden alle Dateien unabhängig von Ihrer Größe geprüft.
Netwerkfreigaben prüfen	**Alle Dateien prüfen**	Alle Dateien, auf die zugegriffen wird, werden unabhängig von ihrem Typ geprüft.
	Nur Applikationen prüfen	Prüft ausschließlich Dateien mit den Dateiendungen: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` und `.nws`.
	Nur Dateien mit folgenden Erweiterungen	Nur die Dateien werden überprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.

- **E-Mail-Datenverkehr prüfen** - prüft alle E-Mail-Nachrichten.

  Die folgenden Optionen sind verfügbar:

Optionen	Beschreibung
Eingehende E-Mails prüfen	Prüft alle eingehenden E-Mails und deren Attachments.
Ausgehende E-Mails prüfen	Prüft alle ausgehenden E-Mails.

- **HTTP Datenverkehr prüfen** - prüft HTTP Datenverkehr.
- **Warnen wenn ein Virus entdeckt wurde** - zeigt eine Warnmeldung an, wenn ein Virus in einer Datei oder E-Mail gefunden wurde.

  Bei einer infizierten Datei zeigt das Fenster für Warnungen den Namen des Virus, den Pfad zur infizierten Datei und die mit ihr durchgeführte Aktion an. Bei einer infizierten E-Mail zeigt das Fenster für Warnungen außerdem Informationen über den Sender und Empfänger an.

  Im Falle eines Verdachts kann ein Assistent aufgerufen werden der Ihnen dabei hilft, verdächtige Dateien zur weiteren Analyse an das Acronis Labor zu senden. Optional können Sie Ihre E-Mail-Adresse angeben, um weitere Informationen zur Analyse zu erhalten.
- **Dateien, die über IM erhalten/gesendet wurden prüfen.** Um Dateien zu prüfen, die Sie über Yahoo Messenger oder Windows Live Messenger erhalten oder senden, markieren Sie die entsprechenden Kontrollkästchen.

Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

17.1.3. Konfigurieren des Active Virus Control

Acronis Internet Security Suite 2010 Active Virus Control bietet Schutz gegen neue Bedrohungen mit unbekannten Signaturen. Er überprüft und analysiert konstant das Verhalten der Anwendungen, die auf Ihrem Computer ausgeführt werden und benachrichtigt Sie, wenn eine Anwendung ein verdächtiges Verhalten aufweist.

Active Virus Control kann so konfiguriert werden, dass Sie informiert werden, wenn eine Anwendung versucht eine möglicherweise schädliche Aktion durchzuführen.



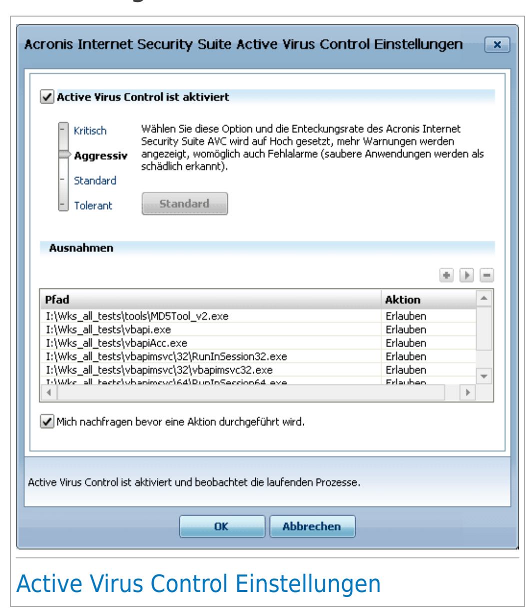
Active Virus Control Warnung

Wenn Sie die entdeckte Anwendung kennen und ihr vertrauen, klicken Sie auf **Erlauben**.

Wenn Sie die Anwendung unverzüglich beenden möchten, klicken Sie auf **OK**.

Wählen Sie **Die Aktion für diese Anwendung merken** aus, bevor Sie Ihre Wahl treffen, und Acronis Internet Security Suite 2010 wird die gleiche Aktion für die entdeckte Anwendung auch in Zukunft ausführen. Die Regel, die erstellt wird, wird in dem Active Virus Control Fenster gelistet.

Um Active Virus Control zu konfigurieren, klicken Sie auf **Fortgeschrittene Einstellungen**.



Active Virus Control Einstellungen

Markieren Sie das dazugehörige Kästchen um Active Virus Control zu ativieren.



Wichtig

Lassen Sie Active Virus Control aktiviert, um gegen unbekannte Viren geschützt zu sein.

Wenn Sie von Active Virus Control benachrichtiget werden wollen, wenn eine Anwendung versucht eine möglicherweise schädliche Aktion durchzuführen, Wählen Sie **Fragen Sie mich nach einer Aktion**.

Sicherheitsstufe einstellen

Die Active Virus Control Sicherheitsstufe ändert sich automatisch, wenn Sie eine neue Stufe für den Echtzeitschutz einstellen. Wenn Sie mit der Standardeinstellung nicht zufrieden sein sollten, können Sie die Sicherheitsstufe manuell konfigurieren.



Anmerkung

Bitte denken Sie daran, dass bei der Änderung der aktuellen Sicherheitsstufe des Echtzeitschutzes, die Sicherheitsstufe der Active Virus Control ebenfalls verändert wird. Wenn Sie die Stufe des Echtzeit-Schutzes auf **Tolerant**, wird Active Virus Control automatisch deaktiviert. In diesem Fall können Sie manuell Active Virus Control aktivieren.

Ziehen Sie den Schieber an der Skala entlang, um die Sicherheitsstufe an Ihre Bedürfnisse anzupassen.

Sicherheitseinstellung	Beschreibung
Wichtig	Strenge Überwachung aller Anwendungen für mögliche böswillige Aktionen.
Standard	Entdeckungsrate ist hoch, somit sind "False Positive" möglich.
Mittel	Anwendungsüberwachung ist angemessen, einige "Fals Positive" sind noch möglich.
Tolerant	Entdeckungsrate ist niedrig und es gibt keine "Fals Positive".

Vertraute / Unzulässige Anwendungen verwalten.

Sie können Anwendungen die Sie kennen und denen Sie vertrauen zur Liste der vertrauenswürdigen Anwendungen hinzufügen. Diese Anwendungen werden nicht länger von der Active Virus Control geprüft, der Zugriff wird automatisch erlaubt.

Die Anwendungen für die eine Regel erstellt wurde, wird in der nachfolgenden Tabelle **Ausnahmen** angezeigt. Der Pfad der Anwendung und die Aktion, die Sie dafür konfiguriert haben (erlaubt oder blockiert) wird für jede Regel angezeigt.

Um die Aktion für eine Anwendung zu ändern, klicken Sie die aktuelle Aktion und wählen eine andere Action.

Um die Liste zu verwalten, benutzen Sie die optionen unter der Tabelle.

- **Hinzufügen** - eine neue Anwendung zur Liste hinzufügen.
- **Entferne** - entfernen Sie eine Anwendung aus der Liste.
- **Editieren** - editiert eine Anwendungsregel.

17.1.4. Echtzeitschutz deaktivieren

Wenn Sie den Echtzeitschutz deaktivieren möchten erscheint ein Warnfenster. Sie müssen die Deaktivierung bestätigen indem Sie wählen wie lange der Schutz deaktiviert werden soll. Zur Auswahl stehen 5, 15 oder 30 Minuten, eine Stunde, permanent oder bis zum nächsten Systemstart.



Warnung

Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen den Echtzeitschutz so kurz wie möglich zu deaktivieren. Während der Echtzeitschutz deaktiviert ist sind Sie nicht vor Schädlingen geschützt.

17.1.5. Antiphishingschutz konfigurieren

Acronis Internet Security Suite 2010 bietet Antiphishingschutz in Echtzeit für:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Sie können den Antiphishingschutz für bestimmte Anwendungen oder komplett deaktivieren.

Sie können auf **Whitelist** klicken um eine Liste von Webseiten zu konfigurieren und verwalten, die nicht von den the Acronis Internet Security Suite 2010 Antiphishing-Engines überprüft werden sollen.



Antiphishing Whitelist

Sie können eine Liste der Webseiten sehen, die Acronis Internet Security Suite 2010 aktuell nicht auf Phishinginhalte prüft.

Um eine neue Webseite zur Whitelist hinzuzufügen geben Sie die Adresse in das Feld **Neue Adresse** ein und klicken Sie dann auf **Hinzufügen**. Die Whitelist sollte nur Webseiten enthalten, denen Sie vollständig vertrauen. Fügen Sie beispielsweise Webseiten hinzu, auf denen Sie häufig einkaufen.



Anmerkung

Mit Hilfe der Acronis Antiphishing-Toolbar in Ihrem Webbrowser können Sie ganz einfach Webseiten zu der Whitelist hinzufügen. Für weitere Informationen lesen Sie bitte *„Integration in Web-Browser“* (S. 273).

Um eine Webseite aus der Whitelist zu entfernen klicken Sie auf die entsprechende Schaltfläche **Entfernen**.

Klicken Sie auf **Speichern** um die Änderungen zu speichern und das Fenster zu schließen.

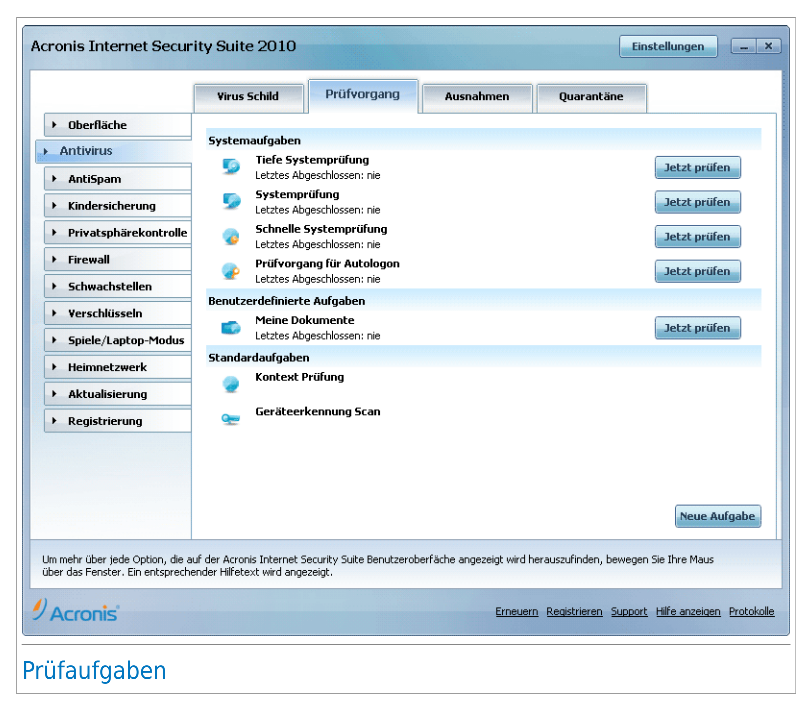
17.2. Prüfvorgang

Die Aufgabe der Acronis Internet Security Suite 2010-Software ist es sicherzustellen, dass es keine Viren in Ihrem System gibt. Dies wird in erster Linie erreicht, indem

Ihre E-Mail-Anhänge und Downloads überprüft und alle Aktionen, die auf Ihrem System stattfinden, überwacht werden.

Es besteht aber die Gefahr, dass ein Virus bereits in Ihrem System ist, bevor Sie Acronis Internet Security Suite 2010 installieren. Deshalb sollten Sie Ihren Computer nach der Installation von Acronis Internet Security Suite 2010 auf residente Viren prüfen. Übrigens sollten Sie Ihren Computer auch in Zukunft häufig auf Viren prüfen.

Um einen On-Demand Prüfvorgang zu konfigurieren und zu starten klicken Sie auf **Antivirus>Prüfen** in der Profiansicht.



Prüfaufgaben

Der Prüfvorgang basiert auf Prüfaufgaben welche die Einstellungen zum Vorgang sowie die zu prüfenden Objekte beinhalten. Sie können den Computer scannen, wann Sie wollen, indem Sie die voreingestellten Aufgaben, oder die von ihnen selbst definierten, starten. Sie können auch einstellen, dass sie regelmässig laufen, oder wenn Ihr System im Leerlauf ist.

17.2.1. Prüfaufgaben

Acronis Internet Security Suite 2010 enthält bereits eine große Zahl von vordefinierten Aufgaben für bestimmte Gegebenheiten. Sie können auch Ihre eigenen benutzerdefinierten Scan-Aufgaben erstellen.

Es gibt drei verschiedene Einstellungen der Prüfoptionen:

- **Systemaufgaben** - Enthält eine Liste von standard Systemeinstellungen. Die folgenen Einstellungen sind möglich:

Standard Einstellungen	Beschreibung
Tiefgehende Systemprüfung	Prüft das komplette System In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Systemprüfung	Prüft alle Dateien mit Ausnahme von Archiven. In der standard Konfiguration, wird nach allen Arten von Malware geprüft, ausser rootkits.
Schnelle Systemprüfung	Prüft die`Windows` und `Programme` Ordner. In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, ausgenommen Rootkits. Ausserdem wird der Arbeitspeicher, die Registy und Cookies nicht geprüft.
Auto-Login Prüfung	Prüft die Objekte, die ausgeführt werden, wenn ein Benutzer sich bei Windows anmeldet. Standardmäßig ist die Prüfung im Hintergrund deaktiviert. Um die Aufgabe zu benutzen, klicken Sie darauf mit der rechten Maustaste, wählen Sie **Planer** und setzen Sie die Ausführung der Aufgabe**beim Systemstart**. Geben Sie an wie lange nach dem Systemstart die Aufgabe gestartet sein wird.(Minuten)



Anmerkung

Da die Prüfvorgänge **Tiefgehende Systemprüfung** und **Systemprüfung** das gesamte System prüfen kann der Vorgang einige Zeit dauern. Daher empfehlen wir Ihnen die Aufgabe mit niedriger Priotität durchzuführen oder wenn Sie das System nicht verwenden.

- **Benutzerdefinierte Aufgaben** - enthält die Anwender definierten Tasks.

  Eine Aufgabe `Meine Dokumente` steht ebenfalls zur Verfügung. Verwenden Sie diese um die folgenden für den jeweiligen Benutzer wichtigen Ordner zu prüfen: `Eigene Dateien`, `Desktop` und `Autostart`. Dies stellt sicher das Ihre Eigenen Dateien, Ihr Desktop und die beim Starten von Windows geladenen Programme schädlingsfrei sind.

- **Standardaufgaben** - enthält eine Liste verschiedener Prüfoptionen. Diese Optionen weisen auf andere Prüfoptionen hin, die in diesem Fenster nicht

ausgeführt werden können. Sie können nur die Einstellungen ändern oder die Prüfberichte ansehen.

Jede Aufgabe hat ein **Eigenschaften** Fenster, welches Ihnen die Konfiguration erlaubt und die Ansicht der Log-Datei. Um dieses Fenster zu öffnen, doppel-klicken Sie die Aufgabe oder klicken Sie den **Eigenschaften** Button. Weitere Informationen finden Sie unter *„Konfiguration einer Prüfaufgabe“* (S. 127).

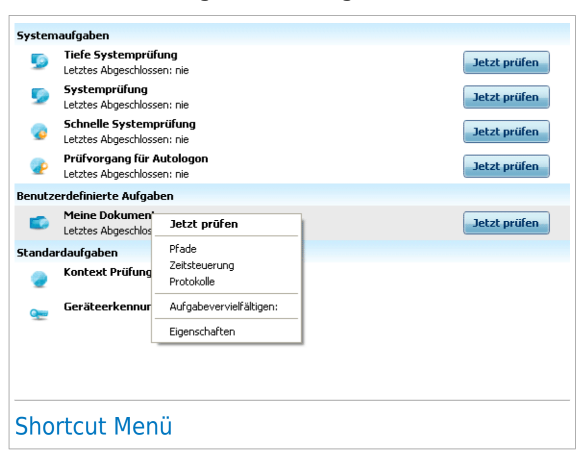
Um einen System- oder Benutzerdefinierten Scan auszuführen, klicken Sie den entsprechenden **Aufgabe Ausführen** Button. Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

Wenn eine Aufgabe konfiguriert ist automatisch zu starten, zu einem späteren Zeitpunkt oder regelmässig, wird der **Planen** Button rechts von der Aufgabe angezeigt. Klicken Sie diesen Button, um das **Eigenschaften** Fenster zu öffnen, Planer Tab, wo Sie die Aufgaben Planung sehen und modifizieren können.

Wenn sie eine erstellte Scan Aufgabe nicht mehr benötigen, können Sie diese löschen, indem Sie den **Löschen** Button, zur rechten der Aufgabe. Sie können system oder sonstige Aufgaben nicht entfernen.

17.2.2. Verwenden des Kontextmenüs

Für jede Aufgabe steht ein Shortcut Menü zur Verfügung. Mit einem rechten Mausklick könne Sie die ausgewählte Aufgabe öffnen.



Shortcut Menü

Für System- und Benutzerdefinierte Aufgaben, sind die folgenden Befehle im Shortcut Menue verfügbar:

- **Jetzt prüfen** - führt die ausgewählte Aufgabe aus und startet eine sofortige Prüfung.

- **Pfad** - Öffnet das **Eigenschaften** Fenster, Reiter Pfad,wo Sie das Prüfziel für die ausgewählte Aufgabe ändern können.



Anmerkung
Im Falle von Systemaufgaben wird diese Option durch **Aufgabenpfade anzeigen** ersetzt.

- **Ablaufplan** - Öffnet das Fenster **Eigenschaften** , Planer, wo Sie die ausgewählten Aufgaben planen können.
- **Protokolle** - Öffnet das Fenster **Eigenschaften** , Protokolle, in welchem Sie die Berichte sehen, die nach dem Prüfungvorgang erstellt wurden.
- **Aufgabe Klonen** - dupliziert die gewählte Aufgabe. Dies ist sinnvoll, wenn neue Aufgaben erstellt werden, weil die Einstellungen für die wiederholte Aufgabe geändert werden können.
- **Löschen** - löscht die ausgewählte Aufgabe.



Anmerkung
Für Systemaufgaben nicht verfügbar. Sie können Systemaufgaben nicht löschen.

- **Eigenschaften** - Öffnet das Fenster **Eigenschaften**, Übersicht, wo Sie die Einstellungen für die ausgewählte Aufgabe ändern können.

Aufgrund ihrer speziellen Beschaffenheit können nur die Optionen **Eigenschaften** und **Berichtsdateien ansehen** unter dem Punkt **Verschiedene Aufgaben** ausgewählt werden.

17.2.3. Erstellen von Zeitgesteuerten Aufgaben

Um eine Prüfaufgabe zu erstellen verwenden Sie eine der folgenden Methoden:

- Klonen einer existierenden Regel, neu benennen und vornehmen der nötigen Änderungen im Fenster Eigenschaften.
- Klicken Sie auf **Neue Aufgabe** um eine neue Aufgabe zu erstellen und zu konfigurieren.

17.2.4. Konfiguration einer Prüfaufgabe

Jede Prüfung hat ihre eigenen **Eigenschaften** ein Fenster indem Sie die prüfoptionen konfigurieren können, das Ziel der Prüfung festlegen,die Tasks planen oder die Berichte ansehen. Um das Fenster zu öffnen klicken Sie auf die **Eigenschaften** Schaltfläche, auf der linken Seite der Aufgabe (oder rechtsklicken Sie die Aufgabe und wählen Sie **Eigenschaften**). Sie können die Aufgabe auch doppel-klicken.



Anmerkung

Weitere Inhalte und Einzelheiten zum Reiter **Protokolle** finden Sie in der Produktbeschreibung unter *„Prüfberichte anzeigen“* (S. 147).

Konfigurieren der Prüfoptionen

Um die Prüfoptionen einer Prüfaufgabe festzulegen klicken Sie mit der rechten Maustaste auf die Aufgabe und wählen Sie **Eigenschaften**. Das folgende Fenster wird erscheinen:



Übersicht

Hier finden Sie Informationen über Aufgaben (Name, letzte Prüfung und geplante Tasks) und können die Prüfeinstellungen setzen.

Prüftiefe festlegen

Sie können die Konfiguration einfach durch das wählen der Prüftiefe festlegen. Ziehen Sie dazu den Zeiger an der Skala entlang, bis Sie das gewünschte Level erreicht haben.

Es gibt 3 mögliche Einstellungen:

Sicherheitseinstellung	Beschreibung
Tolerant	Bietet ausreichende Entdeckung. Belastung der Ressourcen ist niedrig.

Sicherheitseinstellung	Beschreibung
	Nur Programme werden nur auf Viren geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt.
Mittel	Bietet eine gute Entdeckung. Belastung der Ressourcen ist mittel. Alle Dateien werden auf Viren und Spyware geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt.
Aggressiv	Bietet eine hohe Entdeckung. Belastung der Ressourcen ist hoch. Alle Dateien und Archive werden auf Viren und Spyware geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt.

Eine Reihe von allgemeinen Optionen für den Prüfvorgang stehen ebenfalls zur Verfügung:

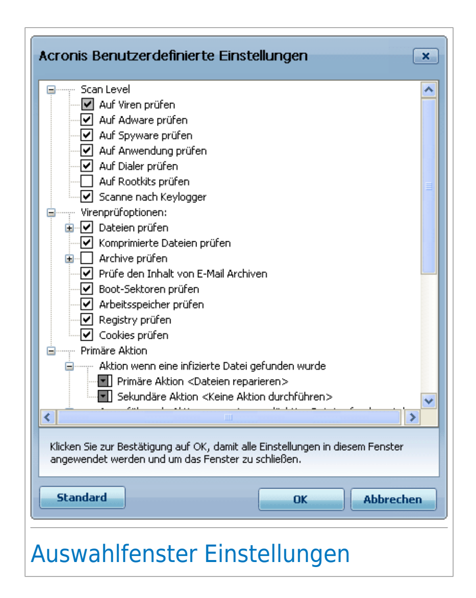
- **Aufgaben mit niedriger Priorität ausführen.** Herabstufung der Priorität des Prüfvorgangs. Andere Programme werden somit schneller ausgeführt. Der gesamte Prüfvorgang dauert damit aber entsprechend länger.
- **Minimiere das Prüffenster zum Sys Tray.** Es verkleinert das Prüffenster beim Prüfvorgang in die untere Symbolleiste. Es kann durch einen Doppelklick auf das Acronis-Icon in der Symbolleiste wieder geöffnet werden.
- **Herunterfahren des Computers nach erfolgtem Prüfvorgang und wenn keine Bedrohungen gefunden wurden**

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

Prüftiefe konfigurieren

Benutzer mit Vorkenntnissen sollten sich die Prüfeinstellungen von Acronis Internet Security Suite 2010 genauer ansehen. Bestimmte Dateierweiterungen, Verzeichnisse und Archive, die wahrscheinlich keine Bedrohung darstellen, können vom Scan ausgeschlossen werden. So wird die Prüfzeit verringert und das Reaktionsvermögen Ihres Rechners während eines Scans verbessert.

Klicken Sie bitte auf **Anpassen** - um Ihre eigenen Prüfoptionen zu setzen. Ein neues Fenster öffnet sich.



Auswahlfenster Einstellungen

Die Prüfoptionen sind wie ein aufklappbares Windows-Explorermenü aufgebaut. Klicken Sie auf "+", um eine Option zu öffnen, und auf "-", um diese zu schließen.

Die Prüfoptionen sind in 3 Kategorien unterteilt:

- **Prüftiefe.** Legen Sie fest nach welcher Art von Schädlingen Acronis Internet Security Suite 2010 suchen soll indem Sie die entsprechende **Prüftiefe** aktivieren.

Optionen	Beschreibung
Dateien prüfen	Sucht nach bekannten Viren. Acronis Internet Security Suite 2010 erkennt auch unvollständige Virenkörper, dadurch wird Ihr System zusätzlich geschützt.
Auf Adware prüfen	Sucht nach möglichen Adware-Anwendungen. Entsprechende Dateien werden wie infizierte Dateien behandelt. Software mit Adware-Komponenten arbeitet unter Umständen nicht mehr, wenn diese Option aktiviert ist.
Auf Spyware prüfen	Sucht nach bekannter Spyware. Entsprechende Dateien werden wie infizierte Dateien behandelt.
Programmdateien prüfen	Legitime Anwendungen prüfen, die als Spionage-Tool verwendet werden können, um schädliche

Optionen	Beschreibung
	Anwendungen oder andere Bedrohungen zu verbergen.
Auf Dialer prüfen	Prüft auf Anwendungen welcher kostenpflichtige Nummern wählen. Erkannte Dateien werden als infiziert behandelt. Dadurch ist es möglich das betroffene Anwendungen nicht mehr funktionsfähig sind.
Auf Rootkits prüfen	Prüft nach versteckten Objekten (Dateien und Prozesse), meist Rootkits genannt.

- **Prüfoptionen.** Geben Sie an, welche Arten von Objekten geprüft werden sollen (Dateitypen, Archive, usw.), indem Sie die entsprechenden Optionen in der Kategorie **Virenprüfoptionen** auswählen.

Optionen		Beschreibung
Dateien	**Alle Dateien prüfen**	Prüft alle vorhanden Dateien.
	Programmdateien	Prüft ausschließlich Dateien mit den Dateiendungen: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml` und `nws`.
	Nur Dateien mit folgenden Erweiterungen	Nur die Dateien werden überprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
Komprimierte Dateien prüfen		Alle komprimierten Dateien werden überprüft.
Archive prüfen		Prüfe innerhalb normaler Archive, so wie `.zip`, `.rar`, `.ace`, `.iso` und Andere. Wählen Sie **Prüfe Installer und chm Archive** auswählen um diesen Dateityp zu prüfen. Die Prüfung archivierter Dateien verlängert die benötigte Zeit für die Prüfung und erfordert mehr Systemressourcen. Sie können Sie Maximalgröße der zu prüfenden Archive

Optionen	Beschreibung
	in Kilobytes (KB) festlegen indem Sie den Wert in dieses Feld eingeben **Limitiere zu prüfende Archivgröße auf**.
Prüfe innerhalb von E-Mail Archiven	Prüft den Inhalt von E-Mails und deren Attachments.
Boot-Sektoren	Prüft die Bootsektoren des Systems.
Speicher prüfen	Prüft den Speicher auf Viren und andere Malware.
Registry prüfen	Prüft Einträge in der Systemregistrierung.
Cookies prüfen	Prüft gespeicherte Cookies von Webseiten.

- **Aktionsoptionen.** Legen Sie die durchzuführende Aktion für jede Kategorie von entdeckten Dateien fest, indem Sie die Optionen in dieser Kategorie verwenden.



Anmerkung

Um eine neue Aktion festzulegen, klicken Sie auf die aktuelle **Erste Aktion** und wählen die gewünschte Option aus dem Menü. Legen Sie eine **Zweite Aktion** fest, die durchgeführt wird, falls die Erste fehlschlägt.

▶ Wählen Sie die durchzuführende Aktion für die erkannten Dateien: Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Keine Aktion durchführen	Es wird keine Aktion für infizierte Dateien ausgeführt. Diese Dateien können Sie in der Berichtsdatei einsehen.
Dateien reparieren	Den Malware-Kode aus den entdeckten infizierten Dateien entfernen.
Dateien löschen	Infizierte Dateien werden ohne Warnung sofort gelöscht.
In die Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

▶ Wählen Sie die durchzuführende Aktion für die als verdächtig erkannten Dateien: Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Keine Aktion durchführen	Es wird keine Aktion für verdächtige Dateien ausgeführt. Diese Dateien finden Sie Berichtsdatei.
Dateien löschen	Die verdächtige Datei wird ohne Warnung sofort gelöscht.
In die Quarantäne verschieben	Verschiebt die verdächtige Datei in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?



Anmerkung

Es wurden verdächtige Dateien gefunden. Wir empfehlen Ihnen diese Dateien zur Analyse an das Acronis Labor zu senden.

- Wählen Sie die durchzuführende Aktion für die erkannten versteckten Dateien (Rootkits): Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Keine Aktion durchführen	Es wird keine Aktion für versteckte Dateien ausgeführt. Diese Dateien finden Sie in der Berichtsdatei.
Dateien umbenennen	Die neue Erweiterung der versteckten Dateien wird `.bd.ren` sein. Infolgedessen werden Sie im Stande sein, zu suchen und solche Dateien auf Ihrem Computer zu finden, falls etwa.
In die Quarantäne verschieben	Verschiebt die versteckten Dateien in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?



Anmerkung

Bitte beachten Sie das es sich bei den versteckten Dateien nicht um die absichtlich von Windows verborgenen Dateien handelt. Die relevanten sind die von speziellen Programmen versteckten, bekannt als Rootkits. Rootkits sind nicht grundsätzlich schädlich. Jedoch werden Sie allgemein dazu benutzt Viren oder Spyware vor normalen Antivirenprogrammen zu tarnen.

- **Option der Vorgehnsweise für passwortgeschützte und verschlüsselte Dateien.** Von Windows verschlüsselten Dateien sind womöglich wichtig für Sie. Deshalb können Sie verschieden Aktionen für infizierte und verdächtige Dateien, die von Windows verschlüsselt sind, konfigurieren. Eine andere

Dateikathegorie welche besondere Vorgehensweisen verlangt sind passwortgeschützte Dateien. Mit Passwörtern geschützte Archive können nicht geprüft werden, außer wenn Sie das Passwort angeben. Verwenden Sie diese Optionen um festzulegen welche Aktionen für passwortgeschützte Archive und Windows-verschlüsselte Dateien vorzunehmen sind.

– **Aktion wenn ein Virus in eine verschlüsselte Datei gefunden wird.** Wählen Sie die anzuwendende Aktion bei von Windows verschlüsselten, infizierten Dateien. Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Keine Aktion durchführen	Zeichne nur infizierte, von Windows verschlüsselte Dateien auf. Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.
Dateien reparieren	Den Malware-Kode aus den entdeckten infizierten Dateien entfernen. Das Desinfizieren kann in manchen Fällen fehlschlagen, beispielsweise wenn die infizierte Datei sich in speziellen Mail-Archiven befindet.
Dateien löschen	Infizierte Dateien direkt und ohne Warnung von der Festplatte entfernen.
In die Quarantäne verschieben	Infizierte Dateien von Ihrer ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

– **Aktion wenn eine verdächtige verschlüsselte Datei gefunden wird.** Wählen Sie die anzuwendende Aktion bei von Windows verschlüsselten, verdächtigen Dateien. Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Keine Aktion durchführen	Zeichne nur verdächtige, von Windows verschlüsselte Dateien auf. Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.
Dateien löschen	Die verdächtige Datei wird ohne Warnung sofort gelöscht.

Aktion	Beschreibung
In die Quarantäne verschieben	Verschiebt die verdächtige Datei in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

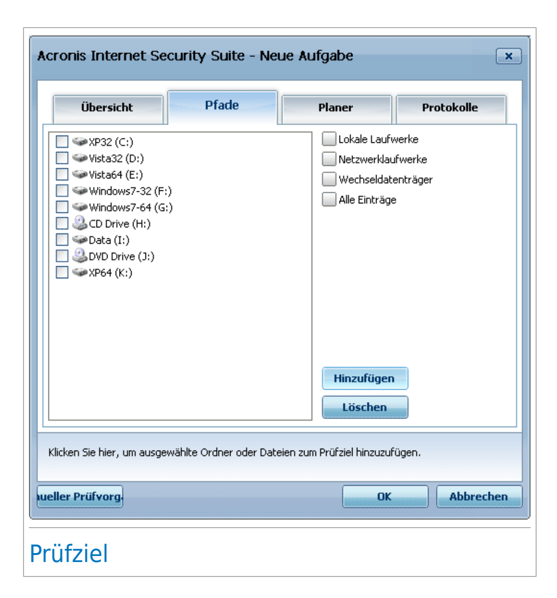
– **Aktion wenn eine passwortgeschützte Datei gefunden wird.** Wählen Sie die durchzuführende Aktion für entdeckte Dateien mit Passwortschutz. Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Nur Log	Nur passwortgeschützte Dateien in das Prüfprotokoll aufnehmen. Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.
Passwort erfragen	Wenn eine passwortgeschützte Datei entdeckt wird, den Benutzer dazu auffordern das Passwort anzugeben, damit die Datei geprüft werden kann.

Mit dem Klick auf **Standard** laden Sie die Grundeinstellungen. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Festlegen der Zielobjekte

Um das Prüfziel einer bestimmten Benutzerprüfaufgabe zu bestimmen, rechtsklicken Sie die Aufgabe und wählen **Pfade**. Alternativ, falls Sie bereits im Eigenschaftenfenster der Aufgabe sind, wählen Sie das **Pfade** Tab. Das folgende Fenster wird erscheinen:



Prüfziel

Sie können die Liste mit Lokalen, Netzwerk und Wechseldatenträgern sowie den Dateien und Ordnern einsehen. Alle markierten Objekte werden beim Prüfvorgang durchsucht.

Folgende Aktionen stehen zur Verfügung:

- **Ornder hinzufügen** - öffnet ein Fenster in dem Sie die zu prüfenden Dateien/Ordner auswählen können.



Anmerkung

Ziehen Sie per Drag & Drop Dateien und Ordner auf die Prüfen-Sektion, um diese der Liste der zu prüfenden Objekte zuzufügen.

- **Entfernen** - Löscht die Datei/denOrdner, die/der zuvor ausgewählt wurde.



Anmerkung

Nur die Dateien/Ordner, die nachträglich hinzugefügt wurden, können gelöscht werden. Dateien/Ordner, die von Acronis Internet Security Suite 2010 vorgegeben wurden, können nicht gelöscht werden.

Ausser dieser Buttons, gibt es weitere Optionen, die das schnelle Auswählen der Scan-Ziele erlauben.

- **Lokale Laufwerke** - prüft die lokalen Laufwerke.
- **Netzlaufwerke** - prüft die verfügbaren Netzwerklaufwerke.

- **Wechseldatenträger** - prüft alle entfernbaren Laufwerke (CD-ROM-Laufwerke, Diskettenlaufwerke, USB-Sticks).
- **Alle Laufwerke** - prüft alle Laufwerke: lokale, entfernbare oder verfügbare Netzwerklaufwerke.



Anmerkung

Zur schnellen Auswahl aller Laufwerke klicken Sie auf **Alle Laufwerke** auswählen.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

Prüfziel der Systemaufgaben anzeigen

Sie können das Prüfziel einer **Systemaufgabe** nicht ändern. Sie können nur ihr Prüfziel sehen.

Um das Zielobjekt einer bestimmten Prüfaufgabe zu sehen, klicken Sie mit der rechten Maustaste auf die Aufgabe und wählen Sie **Aufgabenpfade anzeigen**. Für eine **Systemprüfung**, wird beispielsweise das folgende Fenster erscheinen:



Prüfziel der vollständigen Systemprüfung

Systemprüfung und **Tiefe Systemprüfung** werden alle lokalen Laufwerke prüfen, während **Schnelle Systemprüfung** nur die Ordner `Windows` und `Programme/Dateien` prüfen wird.

Klicken Sie auf **OK**, um dieses Fenster zu schließen. Um den Vorgang auszuführen, klicken Sie auf **Prüfen**.

Zeitgesteuerte Aufgaben festlegen

Bei komplexen Prüfungen kann der Prüfprozess einige Zeit in Anspruch nehmen und läuft am besten, wenn Sei alle anderen Programme schließen. Aus diesem Grunde ist es ratsam die Prüfvorgänge so zu planen, dass Sie Ihren Computer in dieser Zeit nicht nutzen oder er im Standby Modus ist.

Um die Planung einer bestimmten Aufgabe einzusehen oder zu modifizieren, rechtsklicken Sie die Aufgabe und wählen **Planung**. Falls Sie sich bereits im den Eigenschaften der Aufgabe befinden wählen Sie das **Planer** Tab. Das folgende Fenster wird erscheinen:



Planer

Hier können Sie die Einstellungen zum geplanten Prüfvorgang einsehen.

Wenn Sie Prüfvorgänge planen müssen Sie eine der folgenden Optionen auswählen:

- **Nein** - führt den Scan nur auf Anfrage des Nutzers hin durch.
- **Einmal** - führt den Scan nur einmal, zu einem bestimmten Zeitpunkt aus. Definieren Sie den Startzeitpunkt im Feld **Start Datum/Zeit**.
- **Regelmäßig** - führt die Prüfung regelmäßig, in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) aus. Beginnend mit festgelegtem Datum und Uhrzeit.

  Wenn die Prüfung nach einem bestimmten Zeitraum wiederholt werden soll, wählen Sie **Regelmäßig**, und geben Sie in das Textfeld **Alle** die entsprechende Anzahl von Minuten/Stunden/Tage/Wochen/Monate/Jahre ein, nach der die

Wiederholung erfolgen soll. Definieren Sie den Startzeitpunkt im Feld **Start-Datum/Zeit**.

- **Bei Systemstart** - führt die Prüfung nach einer festgelegten Anzahl von Minuten durch, nachdem der Benutzer sich bei Windows angemeldet hat.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

17.2.5. Dateien und Ordner prüfen

Bevor Sie einen Prüfvorgang einleiten sollten Sie sich versichern dass Acronis Internet Security Suite 2010 auf dem neuesten Stand der Maileware-Signaturen ist. Ihren Computer unter Verwendung einer veralteten Signaturendatenbank zu prüfen, kann Acronis Internet Security Suite 2010 daran hindern neue Maleware, welche seit dem letzten Update gefunden wurde, zu erkennen. Überprüfen Sie wann das letzte Update durchgeführt wurde, gehen Sie zu **Aktualisierung>Aktualisierung** in der Profi-Ansicht.



Anmerkung

Damit Sie einen vollständigen Suchlauf mit Acronis Internet Security Suite 2010 durchführen können, ist es wichtig, alle Programme zu beenden. Besonders wichtig ist, dass Sie Ihr E-Mail Programm schließen (z. B. Outlook, Outlook Express oder Eudora).

Prüftips

Hier sind noch einige Prüftips welche Sie vielleicht nützlich finden:

- Je nach Festplattengrösse kann das Durchführen einer umfassenden Systemprüfung (wie Systemprüfung oder Tiefe Systemprüfung) einige Zeit in Anspruch nehmen (bis zu einer Stunde oder mehr). Aus diesem Grund sollten Sie derartige Prüfungen nur durchführen wenn Sie den Computer für eine längere Zeit nicht nutzen (z.B. die Nacht über).

  Sie können die Prüfung planen zu einem günstigen Zeitpunkt zu starten. Stellen Sie sicher den Computer laufen zu lassen. Stellen Sie mit Windows Vista sicher, dass sich Ihr Rechner nicht im Schlafmodus befindet, wenn eine geplante Aufgabe ansteht.

- Falls Sie regelmässig Dateien aus dem Netz in einen bestimmten Ordner herunterladen, erstellen Sie eine neue Prüfaufgabe und legen den Ordner als Prüfziel fest.. Planen sie die Aufgabe ein täglich oder häufiger zu laufen.

- Es gibt eine Malewareart welche sich, durch das Ändern der Windows-Einstellungen, konfiguriert beim Systemstart ausgeführt zu werden. Um Ihren Computer vor derartiger Maleware zu schützen, können Sie die **Autologon Prüfung** beim Systemstart laufen lassen. Bitte beachten Sie das Autologon prüfen die Systemleistung für kurze Zeit nach dem Starten beeinflussen kann.

Prüfoptionen

Acronis Internet Security Suite 2010 bietet vier Arten einen Prüfvorgang durchzuführen:

- Sofortiges Prüfen - Startet die von Ihnen gewählte Aufgabe umgehend
- Kontextbezogenes Prüfen - Rechtsklicken Sie eine Datei oder einen Ordner und wählen Sie **Scanne mit Acronis Internet Security Suite** aus.
- Prüfen per Drag & Drop - verschieben Sie mittels Drag & Drop eine Datei oder einen Ordner auf die Aktivitäts-Anzeige.
- Manuelle Prüfung - Verwenden Sie Acronis Manuelle Prüfung um bestimmte Dateien und Ordner direkt zu prüfen.

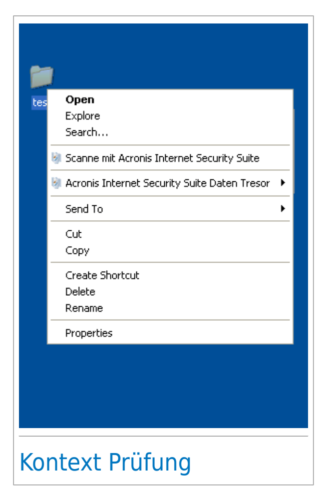
Sofortiges Prüfen

Um Ihren Computer oder Teile Ihres Computers zu prüfen können Sie die Standardeinstellungen nutzen oder Ihre eigenen Aufgaben einrichten. Dies nennt sich Sofortiges Prüfen

Um einen System- oder Benutzerdefinierten Scan auszuführen, klicken Sie den entsprechenden **Aufgabe Ausführen** Button. Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

Scannen mit dem Kontextmenü

Um eine Datei oder einen Ordner zu prüfen ohne eine neue Aufgabe anzulegen können Sie die Kontextmenü-Prüfung verwenden. Dies nennt man Scannen mit dem Kontextmenü



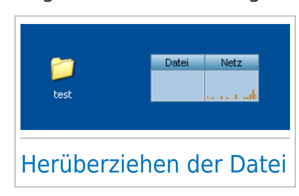
Kontext Prüfung

Rechtsklicken Sie die zu prüfende Datei oder Ordner und wählen **Scanne mit Acronis Internet Security Suite**. Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

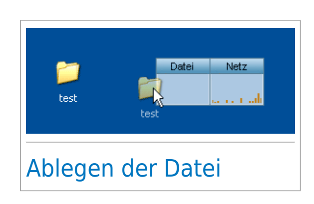
Sie können die Prüfoptionen ändern und die Berichtsdatei einsehen, wenn Sie im Fenster **Eigenschaften** auf **Prüfen Kontext Menü** klicken.

Prüfen per Drag & Drop

Ziehen Sie die gewünschte Datei auf den **Datei-/Netzprüfmonitor**, wie auf den folgenden Bildern dargestellt.



Herüberziehen der Datei



Ablegen der Datei

Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

Manuelle Prüfung

Die Manuelle Prüfung besteht daraus das zu prüfende Objekt direkt über die Acronis Manuelle Prüfungsoption über den Acronis Internet Security Suite 2010 Startmenüeintrag zu wählen.



Anmerkung

Die Manuelle Prüfung ist sehr hilfreich, da Sie diese auch im Abgesicherten Modus von Windows verwenden können.

Um das zu prüfende Objekt auszuwählen verwenden Sie den Pfad: **Start** → **Programme** → **Acronis Internet Security Suite 2010** → **Acronis Manuelle Prüfung**. Das folgende Fenster wird erscheinen:



Manuelle Prüfung

Klicken Sie auf **Ordner hinzufügen**, wählen Sie dann das Ziel dass geprüft werden soll, und wählen Sie **OK**. Wenn Sie mehrere Ordner prüfen möchten, wiederholen Sie diese Aktion für jedes zusätzliches Ziel.

Der Pfad der ausgewählten Position wird in der Spalte **Pfad** angezeigt. Wenn Sie die ausgewählte Position ändern möchten, klicken Sie einfach auf die nebenstehende Schaltfläche **Entfernen**. Klicken Sie auf **Alle entfernen** um alle Ziele die hinzugefügt worden sind, zu löschen.

Wenn Sie fertig sind, klicken Sie **Continue**. Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

Antivirus Prüfassistent

Sobald Sie eine On-Demand-Prüfung starten wird sich der Antivirus-Prüfassistent öffnen. Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.



Anmerkung

Falls der Prüfassistent nicht erscheint, ist die Prüfung möglicherweise konfiguriert still, im Hintergrund, zu laufen. Sehen Sie nach dem Prüffortschritticon im Systemtray. Sie können dieses Objekt anklicken um das Prüffenster zu öffnen und so den Prüffortschritt zu sehen.

Schritt 1/3 - Prüfvorgang

Acronis Internet Security Suite 2010 prüft die gewählten Dateien und Ordner.



Prüfvorgänge durchführen

Sie können den Vorgangsstatus und die Statistiken hierzu sehen (Prüfgeschwindigkeit, vergangene Zeit, Anzahl der geprüften / infizierten / verdächtigen / versteckten Objekte).

Warten Sie bis Acronis Internet Security Suite 2010 den Prüfvorgang beendet hat.



Anmerkung

Der Prüfvorgang kann, abhängig von der Größe Ihrer Festplatte, einen Moment dauern.

Passwortgeschützte Archive. Wenn Acronis Internet Security Suite 2010 während des Prüfvorgangs ein passwortgeschütztes Archiv entdeckt und die Standartaktion ist **Frage nach Passwort**, Sie werden aufgefordert das Passwort anzugeben. Mit Passwörtern geschützte Archive können nicht geprüft werden, außer wenn Sie das Passwort angeben. Die folgenden Optionen sind verfügbar:

- **Passwort.** Wenn Sie möchten das Acronis Internet Security Suite 2010 Archive prüftt, wählen Sie diese Option aus und geben das Passwort an. Falls Sie das Passwort nicht kennen, wählen Sie eine der anderen Optionen.
- **Nicht nach einem Passwort fragen und dieses Objekt bei der Prüfung überspringen.** Wählen Sie diese Optione um das Prüfen diesen Archivs zu überspringen.

- **Alle Passwortgeschützte Datein überspringen ohne diese zu Prüfen.** Wählen Sie diese Option, falls Sie nicht über passwortgeschützte Archive informiert werden möchten. Acronis Internet Security Suite 2010 wird nicht in der Lage sein sie zu prüfen, jedoch wird eine Aufzeichnung im Prüflog eingetragen.

Klicken Sie auf **OK** um fortzufahren.

Stoppen oder pausieren der Prüfung. Sie können den Prüfvorgang jederzeit durch einen Klick auf **Stop&Ja** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten. Um den Prüfvorgang vorrübergehend zu stoppen klicken Sie einfach auf **Pause**. Um den Prüfvorgang fortzusetzen klicken Sie auf **Fortsetzen** .

Schritt 2/3 - Aktionsauswahl

Wenn der Prüfvorgang beendet wurde wird Ihnen ein Fenster angezeigt in welchem Sie eine Zusammenfassung angezeigt bekommen.



Aktionen

Sie bekommen die Anzahl der Risiken welche Ihr System betreffen angezeigt.

Die infizierten Objekte werden in Gruppen angezeigt, je nach Malware, mit der sie infiziert sind. Klicken Sie auf den Link, der der Bedrohung entspricht, um weitere Informationen über die infizierten Objekte zu erhalten.

Sie können eine umfassende Aktion für alle Probleme auswählen oder Sie können einzelne Aktionen für Problemgruppen auswählen.

Eine oder mehrere der folgenden Optionen können im Menu erscheinen:

Aktion	Beschreibung
Keine Aktion durchführen	Es wird keine Aktion für die infizierte Dateien ausgeführt. Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.
Desinfizieren	Den Malware-Code aus den entdeckten infizierten Dateien entfernen.
Löschen	Löscht die infizierten Dateien.
In Quarantäne verschieben	Verschiebt die entdeckten Dateien in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Dateien umbenennen	Die neue Erweiterung der versteckten Dateien wird `.bd.ren` sein. Infolgedessen werden Sie im Stande sein, zu suchen und solche Dateien auf Ihrem Computer zu finden, falls etwa. Bitte beachten Sie das es sich bei den versteckten Dateien nicht um die absichtlich von Windows verborgenen Dateien handelt. Die relevanten sind die von speziellen Programmen versteckten, bekannt als Rootkits. Rootkits sind nicht grundsätzlich schädlich. Jedoch werden Sie allgemein dazu benutzt Viren oder Spyware vor normalen Antivirenprogrammen zu tarnen.

Klicken Sie auf **Fortfahren** um die festgelegten Aktionen anzuwenden.

Schritt 3/3 - Zusammenfassung

Wenn Acronis Internet Security Suite 2010 das Beheben der Risiken beendet hat wird eine Zusammenfassung in einem neuen Fenster geöffnet.



Übersicht

Ihnen wird eine Zusammenfassung angezeigt. Falls Sie umfangreichere Informationen zum Prüfverlauf möchten, klicken Sie **Protokoll** um die Logdatei einzusehen.



Wichtig

Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Säuberungsprozess abgeschlossen werden kann.

Klicken Sie auf **Schließen** um dieses Fenster zu schließen.

Acronis Internet Security Suite 2010 konnte einige Probleme nicht lösen

In den meisten Fällen desinfiziert Acronis Internet Security Suite 2010 erfolgreich die infizierten Dateien, die er entdeckt hat, oder er isoliert die Infektion. Dennoch gibt es Probleme, die nicht gelöst werden können.

In diesen Fällen empfehlen wir Ihnen unser Acronis Support Team unter http://www.acronis.de/support/?ow=1 zu kontaktieren. Die Mitarbeiter unseres Supports werden Ihnen dabei helfen die entsprechenden Probleme zu lösen.

Von Acronis Internet Security Suite 2010 entdeckte verdächtige Dateien

Verdächtige Dateien sind Dateien, die von der heuristischen Analyse als potentiell infiziert erkannt werden, und deren Signaturen noch nicht bekannt sind.

Falls verdächtige Dateien während des Prüfvorganges erkannt werden, werden Sie aufgefordert, diese Dateien zum Acronis-Labor zu senden. Klicken Sie auf **OK** um diese Dateien zum Acronis Lab für weitere Analysen zu senden.

17.2.6. Prüfberichte anzeigen

Um die Prüfberichte nach dem beenden des Prüfvorgangs anzusehen, rechtsklicken Sie auf die Aufgabe und wählen Sie **Protokolle**. Das folgende Fenster wird erscheinen:



Prüfberichte

Hier können Sie die Berichtdateien sehen, die immer dann erstellt werden wenn eine Aufgabe ausgeführt wurde. Jede Datei beinhaltet Informationen über den Status des Prüfprozesses, das Datum und die Zeit wann die Prüfung durchgeführt wurde und eine Zusammenfassung der Prüfergebnisse.

Zwei Schaltflächen sind verfügbar:

- **Löschen** - löscht die ausgewählte Berichtsdatei.
- **Anzeigen** - öffnet die ausgewählte Berichtsdatei. Die Berichtdatei wird in Ihrem Webbrowser geöffnet.

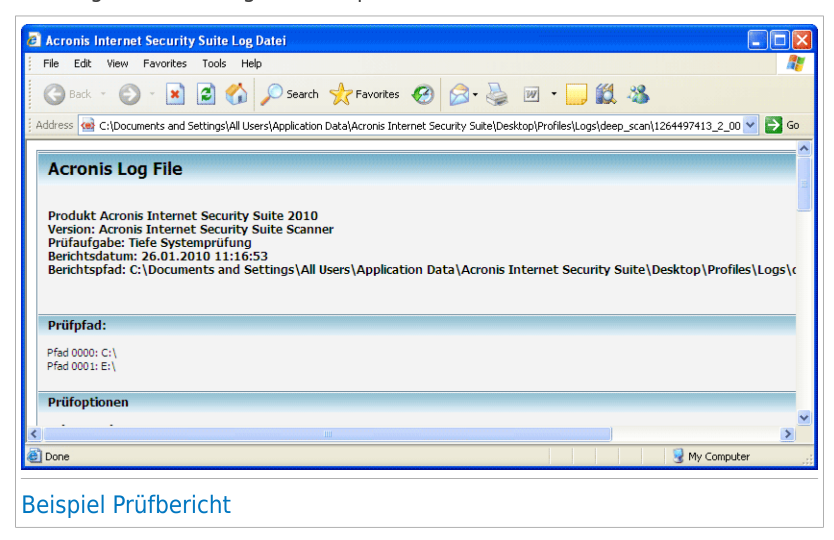


Anmerkung
Sie könne auch um eine Datei anzusehen oder zu löschen einfach mit einem rechten Mausklick die entsprechende Option aus dem Shortcut Menu auswählen.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

Beispiel Prüfbericht

Das folgende Bild zeigt ein Beispiel eines Prüfberichts:



Beispiel Prüfbericht

Der Bericht enthält detaillierte Informationen über den Prüfprozess, so wie Prüfoptionen, das Prüfziel, die entdeckten Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

17.3. Vom Prüfvorgang ausgeschlossene Objekte

In manchen Fällen wird es nötig sein bestimmte Dateien vom Prüfen auszunehmen. Zum Beispiel wenn Sie EICAR Testdateien von der Echtzeiprüfung ausschließen wollen, oder `.avi` Dateien nicht "on-demand" prüfen möchten.

Acronis Internet Security Suite 2010 bietet die Möglichkeit Objekte vom Prüfvorgang, vom Echtzeitschutz oder von beidem auszunehmen. Dies dient dazu die Prüfgeschwindigkeit zu erhöhen oder Eingriffe bei der Arbeit zu verhindern.

Zwei Arten von Objekten können vom Prüfen ausgenommen werden:

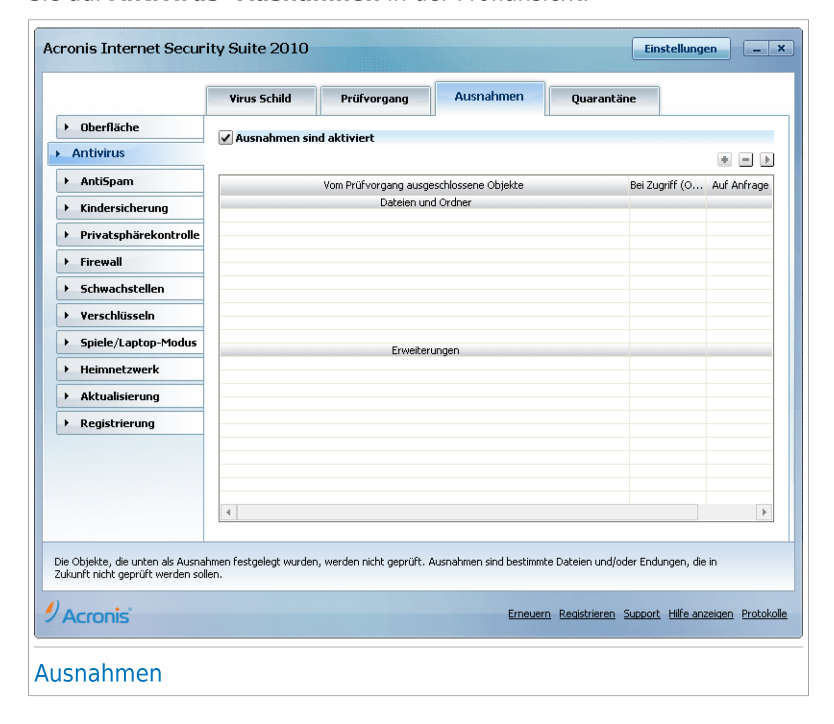
- **Pfade** - Die Datei oder der Ordner (inklusive der enthaltenen Objekte) werden nicht geprüft.
- **Erweiterungen** - Alle Dateien mit der festgelegten Erweiterung werden vom Prüfen ausgeschlossen.



Anmerkung

Die ausgenommenen Objekte werden nicht geprüft, egal ob der Zugriff von Ihnen oder von einem Programm erfolgt.

Um die vom Prüfvorgang ausgeschlossenen Objekte zu sehen und verwalten klicken Sie auf **Antivirus>Ausnahmen** in der Profiansicht.



Ausnahmen

Sie können die Objekte (Dateien, Ordner, Erweiterungen) welche vom Prüfen ausgenommen sind einsehen. Für jedes Objekt ist ersichtlich ob es von der Echtzeitprüfung, dem Prüfvorgang oder beidem ausgenommen ist.



Anmerkung

Die vorgenommenen Ausnahmen werden bei der Kontextmenüprüfung NICHT berücksichtigt. Kontextprüfung ist eine Art von On-Demand-Prüfung: rechtsklicken Sie die zu prüfende Datei oder den Ordner und wählen Sie **Scanne mit Acronis Internet Security Suite** aus.

Um ein Objekt aus der Liste zu entfernen markieren Sie es und klicken Sie dann auf die ⊟ **Entfernen**-Schaltfläche

Um ein Objekt aus der Liste zu bearbeiten, klicken Sie auf die **Bearbeiten**-Schaltfläche. Ein neues Fenster erscheint in welchem Sie die Erweiterung, den Pfad und den Prüftyp der Ausnahme festlegen können. Wenn Sie die Änderungen vorgenommen haben klicken Sie auf **OK**.



Anmerkung
Sie können das Objekt auch mit der rechten Maustaste anklicken un es zu bearbeiten oder zu löschen.

Klicken Sie auf **Verwerfen** um die Änderungen welche Sie noch nicht mit **Übernehmen** bestätigt haben rückgängig zu machen.

17.3.1. Pfade vom Prüfen ausnehmen

Um einen Pfad vom Prüfen auszunehmen klicken Sie auf **Hinzufügen**. Sie werden vom Konfigurationsassistenten durch den Prozess des Ausnehmens geführt.

Schritt 1/4 - Wählen Sie die Objektart

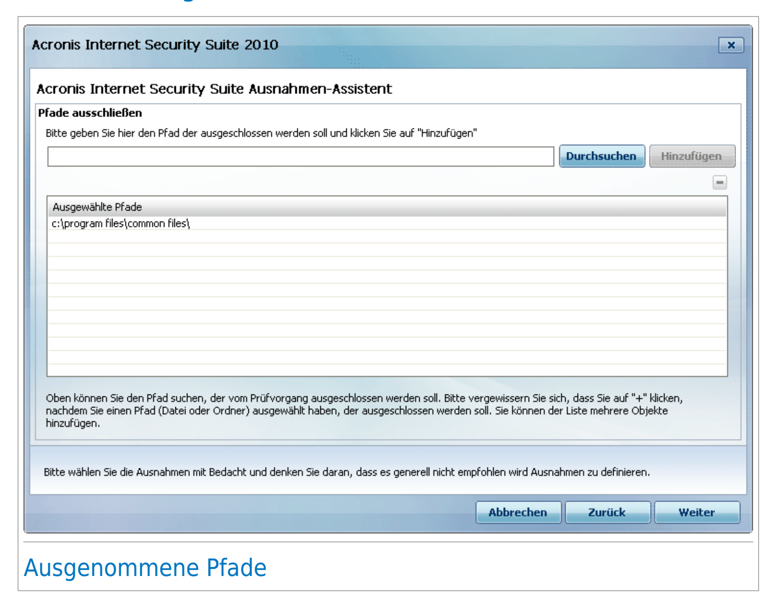


Objektart

Bitte wählen Sie welche Art von Ausnahme Sie erstellen möchten.

Klicken Sie auf **Weiter**.

Schritt 2/4 - Festlegen des Pfads



Ausgenommene Pfade

Um einen Pfad vom Prüfen auszuschliessen verwenden Sie eine von folgenden Methoden:

- Klicken Sie auf **Durchsuchen** und wählen Sie den gewünschten Ordner bzw. Datei, klicken Sie dann auf **Hinzufügen**.
- Geben Sie den Pfad welchen Sie vom Prüfen ausnehmen möchten direkt in das Eingabefeld ein und klicken Sie auf **Hinzufügen**.



Anmerkung

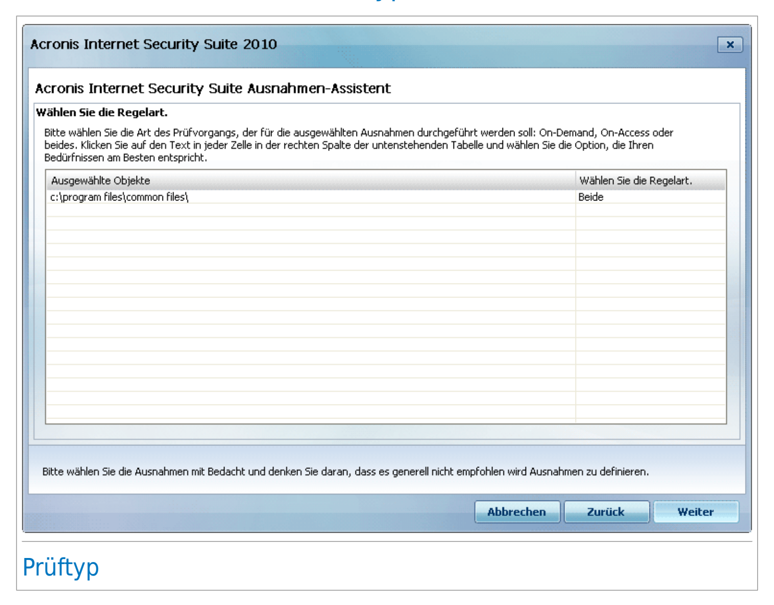
Sollte der eingegebene Pfad nicht existieren so erscheint eine Fehlermeldung. Klicken Sie auf **OK** und prüfen Sie den angegebenen Pfad.

Der Pfad erscheint in dem Moment in der Tabelle in welchem Sie ihn hinzufügen. Sie können so viele Pfade hinzufügen wie Sie wünschen.

Um ein Objekt aus der Liste zu entfernen markieren Sie es und klicken Sie dann auf die ⊟ **Entfernen**-Schaltfläche

Klicken Sie auf **Weiter**.

Schritt 3/4 - Wählen Sie den Prüftyp



Prüftyp

Sie bekommen angezeigt welche Pfade ausgenommen sind und von welchem Prüftyp.

Standardmässig sind die Pfade von beiden Prüftypen ausgenommen, Echtzeitschutz und Prüfvorgang. Um dies zu Ändern klicken Sie auf die entsprechende Anzeige und wählen Sie die gewünschte Option.

Klicken Sie auf **Weiter**.

Schritt 4/4 - Ausgeschlossene Dateien prüfen



Ausgeschlossene Dateien prüfen

Es wird dringend empfohlen die Dateien unter den festgelegten Pfaden zu prüfen, um sicherzustellen, dass diese nicht infiziert sind. Bitte markieren Sie das Kontrollkästchen um diese Dateien zu prüfen, bevor Sie von der Prüfung ausgeschlossen werden.

Klicken Sie auf **Fertigstellen**.

17.3.2. Dateierweiterungen vom Prüfen ausnehmen

Um Dateierweiterungen von der Prüfung auszuschliessen, klicken Sie auf die **Hinzufügen**-Schaltfläche. Der Ausnahmeassistent wird Sie durch den Vorgang begleiten.

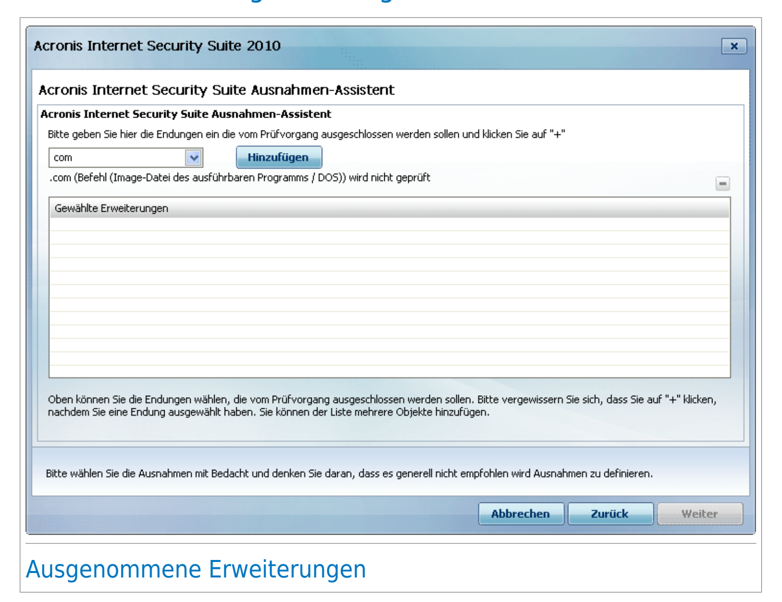
Schritt 1/4 - Wählen Sie die Objektart



Objektart

Wählen Sie die Option um eine Dateierweiterung vom Prüfen auszunehmen. Klicken Sie auf **Weiter**.

Schritt 2/4 - Erweiterungen festlegen



Ausgenommene Erweiterungen

Um die auszunehmenden Erweiterungen festzulegen verwenden Sie eine der folgenden Methoden:

- Wählen Sie die gewünschte Erweiterung aus dem Menü aus und klicken Sie auf **Hinzufügen**.



Anmerkung

Das Menü enthält eine Liste der auf Ihrem System vorhandenen Erweiterungen. Wenn Sie eine Erweiterung auswählen erhalten Sie, falls vorhanden, eine Beschreibung zu dieser.

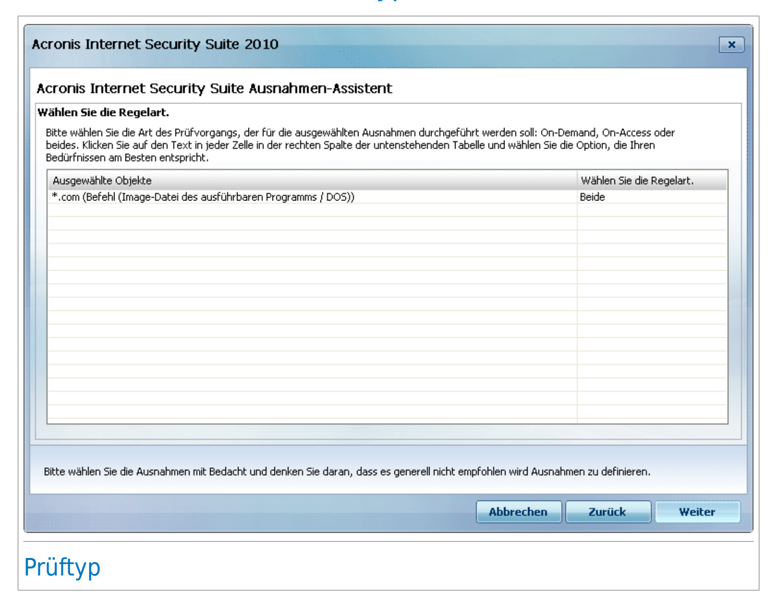
- Geben Sie die gewünschte Erweiterung in das Eingabefeld ein und klicken Sie auf **Hinzufügen**.

Die Erweiterungen erscheinen in der Tabelle sobald Sie diese hinzufügen. Sie können so viele Erweiterungen hinzufügen wie Sie wünschen.

Um ein Objekt aus der Liste zu entfernen markieren Sie es und klicken Sie dann auf die **Entfernen**-Schaltfläche

Klicken Sie auf **Weiter**.

Schritt 3/4 - Wählen Sie den Prüftyp



Prüftyp

Ihnen wird eine Tabelle angezeigt in welche Sie die ausgenommenen Erweiterungen und den Prüftyp einsehen können.

Standardmässig werden die gewählten Erweiterungen von beiden Prüftypen ausgenommen (Echtzeitschutz und Prüfvorgang). Um dies zu klicken Sie auf die entsprechende Spalte und wählen Sie den gewünschten Eintrag.

Klicken Sie auf **Weiter**.

Schritt 4/4 - Wählen Sie den Prüftyp



Prüftyp

Es wird dringend empfohlen die Dateien mit den festgelegten Endungen zu prüfen, um sicherzustellen, dass sie nicht infiziert sind.

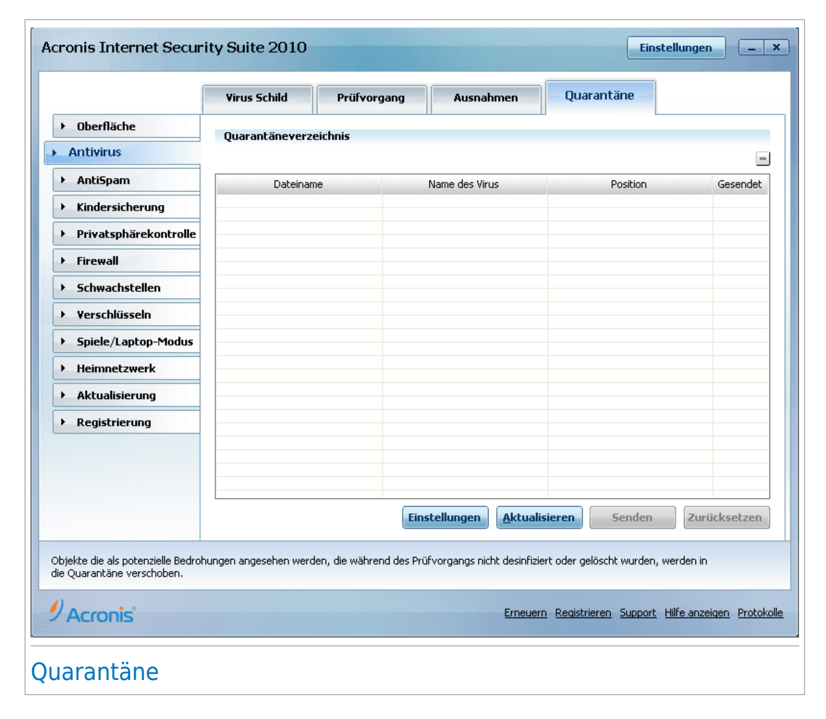
Klicken Sie auf **Fertigstellen**.

17.4. Quarantäne

Acronis Internet Security Suite 2010 ermöglicht die Isolation von infizierten Dateien in einem sicheren Bereich, der so genannten Quarantäne. Durch die Isolation der infizierten Dateien in der Quarantäne reduziert sich das Risiko einer weiteren Infektion. Die infizierten Dateien können zur genaueren Analyse automatisch oder manuell an das Acronis-Labor gesendet werden.

Zudem prüft Acronis Internet Security Suite 2010 nach jedem Malewaresignaturen Update die Datein der Quarantäne. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.

Um die in die Quarantäne verschobenen Dateien zu sehen und Quarantäne-Einstellungen vorzunehmen klicken Sie in der Profiansicht auf **Antivirus>Quarantäne**.



Quarantäne

Der Bereich Quarantäne zeigt alle Dateien an, die sich zur Zeit im Quarantäne-Ordner befinden. Zu jeder Datei die sich in der Quarantäne befindet sind die folgenden Informationen verfügbar: Name der Datei, Name des entdeckten Virus, der ursprüngliche Speicherort und das Übertragungsdatum.



Anmerkung

Die in der Quarantäne enthaltenen Dateien können weder ausgeführt noch geöffnet werden.

17.4.1. Quarantäne-Dateien verwalten

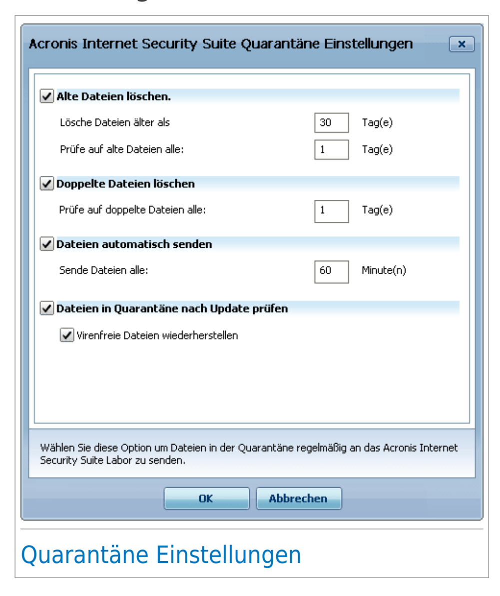
Sie können jede ausgewählte Datei aus der Quarantäne in das Acronis labor senden in dem Sie **Senden** klicken. Standardmässig überträgt prüft Acronis Internet Security Suite 2010 die Dateien in Quarantäne alle 60 Minuten.

Um eine Datei aus der Quarantäne zu löschen klicken Sie **Entfernen** button. Wenn Sie eine infizierte Datei an ihrem originalen Speicherort wiederherstellen wollen klicken Sie **Wiederherstellen**.

Kontextmenü. Um die Quarantänedateien einfach zu verwalten steht ein Kontextmenü zur Verfügung. Hier stehen die selben Option wie zuvor genannt zur Verfügung. Klicken Sie auf **Aktualisieren** um die Ansicht zu erneuern.

17.4.2. Quarantäne-Einstellungen konfigurieren

Wenn Sie die Quarantäne-Einstellungen konfigurieren möchten klicken Sie auf **Einstellungen**. Ein neues Fenster wird sich öffnen.



Quarantäne Einstellungen

Über die Quarantäne-Einstellungen können Sie folgende Aktionen festlegen:

Alte Dateien löschen. Um alte Dateien in der Quarantäne automatisch zu löschen aktivieren Sie die entsprechende Option. Sie können festlegen nach wievielen Tagen alte Dateien gelöscht werden und wie oft Acronis Internet Security Suite 2010 dies prüfen soll.



Anmerkung

In der Standardeinstellungen prüft Acronis Internet Security Suite 2010 jeden Tag nach alten Dateien und löscht diese wenn Sie älter als 30 Tage sind.

Doppelte Dateien löschen. Um doppelte Dateien in der Quarantäne automatisch zu löschen aktivieren Sie die entsprechende Option. Geben Sie an wie oft eine Prüfung erfolgen soll.



Anmerkung

Standardmässig prüft Acronis Internet Security Suite 2010 die Dateien in Quarantäne einmal täglich auf Dublikate.

Dateien automatisch senden. Um Dateien automatisch an das BitDefender Labor zu senden aktivieren Sie diese Option. Geben Sie an wie oft BitDefender die Dateien sendet.



Anmerkung

Standardmässig überträgt prüft Acronis Internet Security Suite 2010 die Dateien in Quarantäne alle 60 Minuten.

Dateien in der Quarantäne nach einem Update nochmals prüfen. Um Dateien in der Quarantäne nach einem Update nochmals prüfen zu lassen aktivieren Sie die entsprechende Option. Sie können gereinigte Dateien automatisch an ihrem ursprünglichen Speicherort wiederherstellen, indem Sie **Saubere Dateien wiederherstellen** wählen.

Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

18. AntiSpam

Acronis Antispam verwendet aussergewöhnliche Technologische Innovationen und Standard-Antispam Filter um Spam auszusortieren bevor dieser im Posteingang landet.

18.1. Antispam Einblicke

Spam ist ein wachsendes Problem für Heimanwender wie auch für Organisationen. Sie wollen wahrscheinlich nicht, dass Ihre Kinder die meisten dieser Spam-Mails mit häufig pornographischem Inhalt lesen oder dass Sie deswegen sogar in Unannehmlichkeiten geraten. Spam wird immer mehr zum Ärgernis. Daher ist es das Beste, diese Mails gar nicht mehr zu erhalten.

18.1.1. Antispam Filter

Die Acronis Internet Security Suite 2010 Antispam Engine arbeitet mit verschiedenen Filtern, die sicherstellen, dass Ihr Posteingang spamfrei bleibt: Freundesliste, Spammerliste, Charsetfilter, Bildfilter, URL-Filter, NeuNet (Heuristischer) Filter und Bayesianischer Filter.



Anmerkung

Sie können jeden dieser Filter im der Reiter Einstellungen der **Antispam** Sektion aktivieren/deaktivieren.

Liste der Freunde/Liste der Spammer

Viele Menschen kommunizieren normalerweise mit einer bestimmten Gruppe von Menschen oder aber erhalten Nachrichten von Firmen oder Organisationen mit derselben Domain. Wird eine **Liste der Freunde bzw. Spammer** geführt, so können Sie festlegen, welche E-Mails Sie erhalten wollen (die von Freunden) und welche Sie nicht erhalten möchten (die von Spammern).

Sie können die Listen der Freunde/Spammer über die Profiansichtoder in der Antispamleiste verwalten, die einige der meist benutzten Mail-Clients miteinbezieht.



Anmerkung

Wir empfehlen, dass Sie die Namen Ihrer Freunde und deren E-Mail-Adressen der **Freundesliste** hinzufügen, damit sichergestellt ist, dass nur solche E-Mails an Sie weitergeleitet werden.

Zeichensatz-Filter

Viele der Spam-Mails sind in Kyrillisch und/oder Asiatisch geschrieben. Der Schriftsatz-Filter erkannt diese Art von Nachrichten und behandelt diese als SPAM.

Grafik-Filter

Seit es eine Herausforderung geworden ist, heuristische Filtermethoden zu vermeiden, sind Posteingänge heutzutage mehr und mehr mit Nachrichten angefüllt, die lediglich aus einem Bild mit unerwünschten Inhalt bestehen. Um mit diesem wachsenden Problem zurechtzukommen, vergleicht der **Image-Filter** die Bildsignatur aus der E-Mail mit denen aus der Datenbank von Acronis Internet Security Suite 2010. Im Fall einer Übereinstimmung wird die E-Mail als SPAM gekennzeichnet.

URL-Filter

Viele Spam-Mails enthalten Links zu verschiedenen Webseiten (der Inhalt ist meist kommerziell). In der BitDefender-Datenbank sind diese Links aufgeführt.

Diese Datenbank wird von Acronis ständig aktuell gehalten. Der URL-Filter prüft jede URL in einer Nachricht und vergleicht Sie mit der Datenbank. Sollten die URLs übereinstimmen wird die Nachricht als SPAM markiert.

NeuNet-Filter (Heuristik)

Der **Heuristischer Filter** führt eine Reihe von Tests mit allen Nachrichtinhalten durch (z. B. wird nicht nur die Betreffzeile, sondern auch der Nachrichtentext auf HTML-Text überprüft), hält Ausschau nach Wörtern, Phrasen, Links oder anderen Charakteristiken von Spam. Basierend auf dem Resultat der Analyse wird ein SPAM Wert hinzugefügt.

Der Filter erkennt auch Nachrichten welche im Betreff als `Ausdrücklich Sexuel` markiert wurden und markiert diese als SPAM.



Anmerkung

Seit dem 19. Mai 2004 müssen E-Mails mit sexuellem Inhalt entsprechend markiert werden `Sexual ausdrücklich:` und in der Betreffzeile muss explizit auf den Inhalt hingewiesen werden.

Bayesian-Filter

Der **Bayesian-Filter** klassifiziert Nachrichten an Hand von statistischen Informationen bezüglich spezieller Wörter, die in den Nachrichten auftauchen, als Spam oder Nicht-Spam (nach Ihren Vorgaben oder dem heuristischen Filter).

Das bedeutet zum Beispiel, dass es, wenn ein bestimmtes Wort mehrfach erscheint, sich mit hoher Wahrscheinlichkeit um Spam handelt. Alle relevanten Wörter innerhalb einer Nachricht werden einbezogen.

Dieser Filter bietet eine weitere interessante Charakteristik: Er ist lernfähig. Er speichert Informationen einer empfangenen Nachricht eines bestimmten Nutzers. Um korrekt zu funktionieren, benötigt der Filter Training, was bedeutet, dass er mit Mustern von legitimen Nachrichten gefüllt werden sollte. Ab und zu muss der Filter

aktualisiert werden, besonders dann, wenn er eine falsche Entscheidung getroffen hat.



Wichtig

Sie korrigieren den bayesianischen Filter, indem Sie die **Ist Spam** und **Kein Spam** -Schaltflächen in der Antispam Toolbar benutzen.

18.1.2. Antispam Vorgang

Die Acronis Internet Security Suite 2010 Antispam Engine benutzt alle Antispam Filter kombiniert um festzustellen ob eine bestimmte E-Mail in die **Inbox** gelangen sollte, oder nicht.



Wichtig

Spams die Acronis Internet Security Suite 2010 entdeckt, werden markiert dem `[SPAM]` Prefix in der Betreffzeile. Acronis Internet Security Suite 2010 legt Spam-Nachrichten automatisch in einem festgelegten Ordner ab, wie folgt:

- In Microsoft Outlook, Spams werden verschoben in den **Spam** Ordner, zu finden unter **gelöschte Objekte**. Der **Spam** Ordner wurde während der Installation von Acronis Internet Security Suite 2010 erstellt.
- In Outlook Express und Windows Mail, werden Spams direkt in **gelöschte Objekte** verschoben.
- Im Mozilla Thunderbird, werden Spams in den **Spam** Ordner verschoben, der unter **Trash** Ordner zu finden ist. Der **Spam** Ordner wurde während der Installation von Acronis Internet Security Suite 2010 erstellt.

Falls Sie andere E-Mail Clients verwenden, so müssen Sie eine Regel erstellen um Nachrichten die als `[SPAM]` markiert sind, in einen eigens erstellten Ordner zu verschieben.

Jede E-Mail, die aus dem Internet kommt, wird zuerst mit den Filtern Freundesliste/Spammerliste überprüft. Falls der Sender in der Freundesliste gefunden wird, wird diese Mail direkt in Ihren **Posteingang** gesendet.

Der Filter Liste der Spammer überprüft, ob der Absender der E-Mail auf der gleichnamigen Liste eingetragen ist. Falls dem so ist, wird die Mail markiert und in den **Spam**-Ordner verschoben (zu finden bei Microsoft Outlook).

Der Zeichensatz-Filter überprüft, ob die E-Mail in Kyrillisch oder mit asiatischen Buchstaben geschrieben worden ist. Falls dem so ist, wird die Mail markiert und in den **Spam**-Ordner verschoben.

Falls die E-Mail diese Merkmale nicht aufweist, wird sie mit dem Grafik-Filter überprüft. Die **Grafik-Filter** erkennt E-Mail-Nachrichten, die Bilder bzw. Grafiken und Spam-Inhalte beinhalten.

Der URL-Filter überprüft die E-Mail nach Links und vergleicht diese mit jenen, die in der Acronis Internet Security Suite 2010-Datenbank stehen. Im Falle eines Treffers wird diese E-Mail als Spam verschoben.

Der Heuristische Filter testet die E-Mail auf den Inhalt, sucht nach Wörtern, Phrasen, Links oder anderen Charakteristiken von Spam. Im Falle eines Treffers wird auch hier die E-Mail zum Spam hinzugefügt.



Anmerkung

Falls in der Betreffzeile Wörter mit sexuellem Inhalt gefunden werden, markiert Acronis Internet Security Suite 2010 die E-Mail als Spam.

Der Bayesian-Filter analysiert die Nachricht aufgrund statistischer Informationen in Bezug auf spezielle Wörter und vergleicht diese mit denen, die nicht als Spam klassifiziert sind. Das Ergebnis ist das Hinzufügen eines Spam-Score in die E-Mail.

Falls die Summe aller Treffer (URL-Treffer + Heuristischer Treffer + Bayesian Treffer) die Spam-Treffer übersteigt (die durch den Benutzer in der Antispam-Sektion als Toleranzniveau festgelegt wird), wird die E-Mail als Spam deklariert.

18.1.3. Antispam Updates

Bei jedem durchgeführten Update werden:

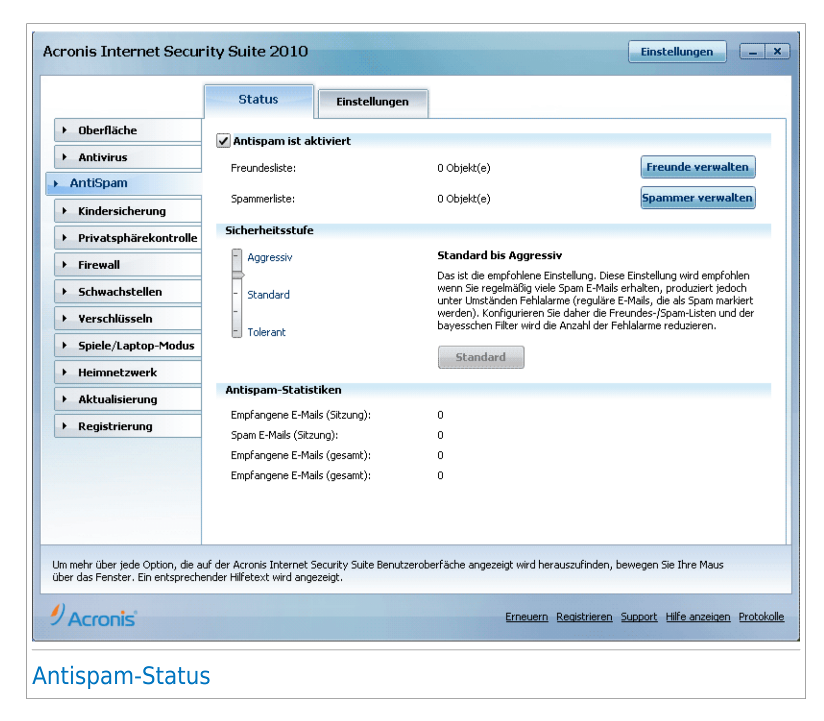
- werden neue Bildsignaturen zum **Grafik-Filter** hinzugefügt.
- werden neue Links zum **URL-Filter** hinzugefügt.
- werden dem **Heuristik-Filter** neue Regeln hinzugefügt.

Somit wird die Effektivität des AntiSpam-Moduls laufend verbessert.

Acronis Internet Security Suite 2010 kann automatische Updates durchführen. Lassen Sie daher das **Automatische Update** aktiviert.

18.2. Status

Um den Antispam-Schutz zu konfigurieren wählen Sie **Antispam>Status** in der erweiterten Ansicht.



Antispam-Status

Sie können sehen ob Antispam aktiviert oder deaktiviert ist. Wenn Sie den Antispam-Status verändern möchten, markieren Sie die entsprechende Option oder lassen Sie sie frei.



Wichtig

Um zu verhindern, dass Spam in Ihren **Posteingang** gelangt, aktivieren Sie die **Antispam Filter**.

In der **Statistiken**-Sektion erhalten Sie einen Einblick in die Statistiken des AntiSpam-Moduls. Die Ergebnisse werden pro Sitzung (seitdem Sie Ihren Computer gestartet haben) angezeigt. Sie können aber auch einen Überblick seit der Installation der AntiSpam-Filter bekommen.

18.2.1. Sicherheitsstufe anpassen

Sie können die Sicherheitseinstellung an Ihre Anforderungen anpassen. Ziehen Sie die Anzeige auf der Scala auf die richtige Einstellung.

Es gibt 5 Sicherheitsstufen:

Sicherheitseinstellung	Beschreibung
Tolerant	Bietet Schutz für E-Mail Accounts, die eine Menge von erlaubter kommerzieller E-Mail erhalten. Der Filter wird den meisten E-Mail Verkehr zulassen, aber möglicherweise falsche E-Mails durchlassen (Spam eingeordnet als erlaubte Mail)
Tolerant bis Mittel	Bietet Schutz für E-Mail Accounts, die ein paar erlaubte kommerzielle E-Mails erhalten. Der Filter wird den meisten E-Mail Verkehr zulassen, aber möglicherweise falsche E-Mails durchlassen (Spam eingeordnet als erlaubte Mail)
Mittel	Bietet Schutz für reguläre Accounts. Der Filter blockiert die meisten Spam Mails und vermeidet Fehlalarme.
Mittel bis aggressiv	Bietet Schutz für E-Mail Accounts, die regelmäßig ein hohes Volumen an Spam erhalten. Der Filter läßt extrem wenig Spam durch, aber es kann zu Fehlalarmen kommen indem erlaubte Mails als Spam gekennzeichnet werden. Konfigurieren der **Freunde/Spammer Liste** und Training des **Bayesian Filters** um die Anzahl an Fehlalarmen zu reduzieren.
Aggressiv	Bietet Schutz für E-Mails Accounts, die regelmäßig eine hohe Zahl an Spam Mails erhalten. Der Filter läßt extrem wenig Spam durch, aber es kann zu Fehlalarmen kommen indem erlaubte Mails als Spam gekennzeichnet werden. Fügen Sie Ihre Kontakte zur **Freundesliste** hinzu, um die Anzahl an Fehlalarmen zu reduzieren.

Sie können das Level für den gewünschten Schutz einstellen. (**Moderat zu Aggressiv**)Klicken Sie **Level anpassen**.

18.2.2. Freundesliste konfigurieren

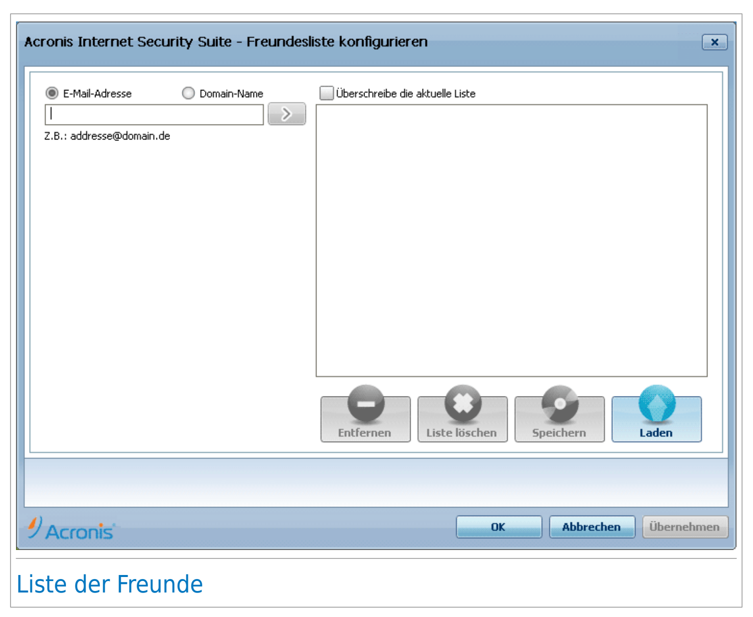
Liste der Freunde – die Liste aller E-Mail-Adressen, von denen Sie immer Mails erhalten wollen, egal welchen Inhalts diese sind. Nachrichten Ihrer Freunde werden nicht als Spam deklariert, auch wenn der Inhalt dem von Spam ähnlich sein sollte.



Anmerkung

Jede Mail von einer Adresse Ihrer **Freundesliste** wird automatisch in Ihren Posteingang verschoben.

Um die Freundesliste zu konfigurieren, klicken Sie auf **Freunde verwalten** (oder klicken Sie auf die Schaltfläche **Freunde** in der Antispam Toolbar).



Liste der Freunde

Hier können Sie die Einträge Ihrer **Freundesliste** ändern.

Falls Sie eine E-Mail-Adresse hinzufügen möchten, kontrollieren Sie die **E-Mail-Adresse**, tragen Sie sie ein und klicken Sie auf den ⊠-Button. Die Adresse wird Ihrer **Freundesliste** hinzugefügt.



Wichtig

Syntax: name@domain.com.

Falls Sie eine Domain hinzufügen möchten, kontrollieren Sie diese und schreiben Sie sie in das Feld **Domänen-Name**; klicken Sie auf den ⊠-Button. Die Domain wird Ihrer **Freundesliste** hinzugefügt.



Wichtig

Syntax:

- @domain.com, *domain.com und domain.com - alle eingehenden Mails von domain.com werden in Ihren **Posteingang** verschoben, gleich welchen Inhalts;
- *domain* - alle eingehenden Mails von domain werden ohne Überprüfung Ihres Inhaltes in Ihren **Posteingang** verschoben, gleich welchen Inhalts;
- *com - alle Mails mit der Endung com werden in Ihren **Posteingang** verschoben, gleich welchen Inhalts;

Um einen Eintrag aus der Liste zu entfernen markieren Sie diesen und klicken Sie dann auf **Entfernen**. Um alle Einträge zu löschen, klicken Sie auf **Liste löschen** und danach auf **Ja** um dies zu bestätigen.

Sie können die Liste der Freunde speichern, so das diese auf einen anderen Rechner oder nach einer neuinstallation benutzt werden kann. Um die Freundesliste zu speichern klicken Sie auf **Speichern** und speichern sie diese an den gewünschten Ort. Die Datei wird `.bwl` als Erweiterung haben.

Um eine zuvor gespeicherte Freundesliste zu laden, klicken Sie **Laden** und öffnen die entsprechende `.bwl` Datei. Um den Inhalt einer aktuellen Liste zurückzusetzen während der Inhalt einer zuvor gespeicherten Liste geladen wird, wählen Sie **Liste beim Laden leeren**.



Anmerkung

Wir empfehlen, dass Sie die Namen Ihrer Freunde und deren E-Mail-Adressen der **Freundesliste** hinzufügen, damit sichergestellt ist, dass nur solche E-Mails an Sie weitergeleitet werden.

Klicken Sie auf **Übernehmen** und **OK**, um zu speichern und um die **Freundesliste** zu schließen.

18.2.3. Konfigurieren der Spammerliste

Liste der Spammer - Liste die alle E-Mail-Adressen enthält, von denen Sie keine Nachrichten erhalten wollen, gleich welchen Inhalts.



Anmerkung

Jede Mail von einer Adresse Ihrer **Spammerliste** wird automatisch in Ihren Papierkorb verschoben.

Um die Spammerliste zu konfigurieren, klicken Sie auf **Spammer verwalten** (oder klicken Sie auf die Schaltfläche **Spammer** in der Antispam Toolbar).



Liste der Spammer

Hier können Sie die Einträge Ihrer **Spammerliste** ändern.

Falls Sie eine E-Mail-Adresse hinzufügen möchten, kontrollieren Sie die **E-Mail-Adresse**, tragen Sie sie ein und klicken Sie auf den ⊡-Button. Die Adresse wird Ihrer **Spammerliste** hinzugefügt.



Wichtig

Syntax: name@domain.com.

Falls Sie eine Domain hinzufügen möchten, kontrollieren Sie diese und schreiben Sie sie in das Feld **Domänen-Name**; klicken Sie auf den ⊡-Button. Die Domain wird Ihrer **Spammerliste** hinzugefügt.



Wichtig

Syntax:

- @domain.com, *domain.com und domain.com - alle eingehenden Mails von domain.com werden als Spam markiert;
- *domain* - alle eingehenden Mails von domain (egal welcher Endung) werden als Spam markiert;
- *com - alle Mails mit dieser Endung com werden als Spam markiert.



Warnung

Fügen Sie keine legitime Webbasierte E-Mail Anbieter (wie: Yahoo, Gmail, Hotmail oder andere) zu der Spammerliste hinzu. Andernfalls werden die E-Mail-Nachrichten, die von jedem möglichem Benutzer solch eines Anbieters gesendet werden, als Spam eingestufft. z.B: wenn Sie `yahoo.com` zu Spammerliste hinzufügen, werden alle E-Mails die von `yahoo.com` Adressen kommen, als `[spam]` markiert.

Um einen Eintrag aus der Liste zu entfernen markieren Sie diesen und klicken Sie dann auf **Entfernen**. Um alle Einträge zu löschen, klicken Sie auf **Liste löschen** und danach auf **Ja** um dies zu bestätigen.

Sie können die Spammer Liste in eine Datei sichern, damit Sie sie nach einer Neuinstallation oder auf einem anderen Computer nutzen können. Um die Spammerliste zu speichern klicken Sie auf **Speichern** und speichern sie diese an den gewünschten Ort. Die Datei wird `.bwl` als Erweiterung haben.

Um eine zuvor gespeicherte Spammerliste zu laden, klicken Sie **Laden** und öffnen die entsprechende `.bwl` Datei. Um den Inhalt einer aktuellen Liste zurückzusetzen während der Inhalt einer zuvor gespeicherten Liste geladen wird, wählen Sie **Liste beim Laden leeren**.

Klicken Sie auf **Übernehmen** und **OK**, um zu speichern und um die **Spammerliste** zu schließen.

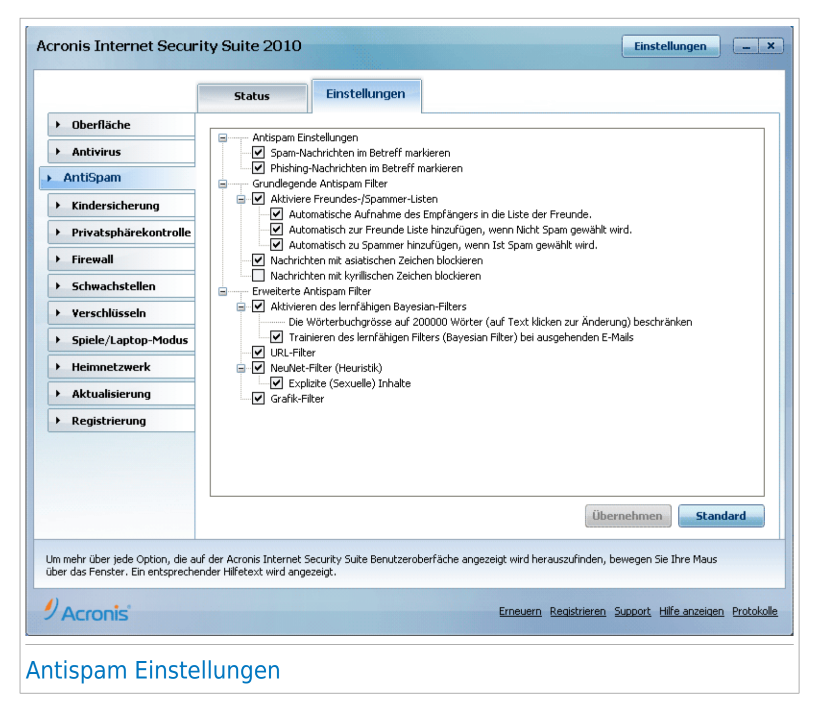


Wichtig

Wenn Sie Acronis Internet Security Suite 2010 erneut installieren möchten, sollten sie Ihre **Freundes -** / **Spammerliste** speichern und nach der Neuinstallation wieder laden.

18.3. Einstellungen

Um die Antispam Einstellungen und Filter zu konfigurieren klicken Sie auf **Antispam>Einstellungen** in der Profiansicht



Antispam Einstellungen

Drei Kategorien von Einstellungen sind möglich (**Allgemein**, **Erweitert** und **Antispam Filter**). Sie sind erweiterbar wie ein Menü, vergleichbar mit denen von Windows.



Anmerkung

Klicken Sie auf eine Box mit einem "+", um ein Menü auszuklappen, und auf ein "-", um es zu schließen.

Um einen Filter zu (de)aktivieren setzen bzw. entfernen Sie das jeweilige Häkchen in der Checkbox.

Wenn Sie die Standardeinstellungen anwenden möchten, klicken Sie auf **Standard**.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

18.3.1. Antispam Einstellungen

- **Spam-Nachrichten im Betreff markieren** - alle E-Mails, die als SPAM Mails eingestuft werden, erhalten eine SPAM-Markierung in der Betreffzeile.

- **Phishing (Schutz vor Diebstahl von Zugangsdaten) Nachrichten im Betreff kennzeichnen** - alle E-Mails, die als Phishing Mails eingestuft werden, erhalten eine SPAM-Markierung in der Betreffzeile.

18.3.2. Grundlegende Antispam Filter

- **Freundes/Spammer listen** - aktiviert/deaktiviert den Freundes/Spammerliste;
  - **Zur Liste der Freunde hinzufügen** - um die Sender in Ihre Freundesliste übernehmen.
  - **Automatisch zur Liste der Freunde hinzufügen** - wird beim nächsten Klick auf den **Kein Spam**-Button in der Antispam Toolbar den Sender automatisch zu Liste der Freunde hinzufügen.
  - **Automatisch zur Liste der Spammer hinzufügen**- wird beim nächsten Klick auf den **Ist Spam**-Button in der Antispam Toolbar den Sender automatisch zu Liste der Spammer hinzufügen.



Anmerkung

Die **Kein Spam** und **Ist Spam**- trainieren den Bayesian Filter.

- **Asiatische Zeichen blockieren** - blockiert Nachrichten mit Asiatischen Zeichen.
- **Kyrillische Zeichen blockieren** - blockiert Nachrichten mit Kyrillischen Zeichen.

18.3.3. Erweiterte Antispam Filter

- **Bayesian Filter** - aktiviert/deaktiviert den Bayesian Filter;
  - **Wörterbuch auf 200.000 Wörter beschränken** - mit dieser Option können Sie die Größe des bayesianischen Verzeichnisses begrenzen – kleiner ist schneller, größer ist akkurater.



Anmerkung

Die empfohlene Größe sind 200.000 Wörter.

  - **Trainieren des Bayesian Filter für ausgehende E-Mails** - trainieren des Bayesian Filter für ausgehende E-Mails.
- **URL Filter** - aktiviert/deaktiviert den URL Filter;
- **Heuristischer Filter** - aktiviert/deaktiviert den Heuristischer Filter;
  - **Explizite (Sexuelle) Inhalte** - aktiviert/deaktiviert den Filter für eindeutige Inhalte;
- **Grafik-Filter** - aktiviert/deaktiviert den Filter für Bilder bzw. Grafiken.

19. Kindersicherung

Die Kindersicherung gibt Ihnen die Möglichkeit den Zugriff auf das Internet und auf bestimmte Programme für jeden Benutzer mit einem Benutzerkonto auf dem System zu kontrollieren.

Sie können die Kindersicherung so konfigurieren, dass Folgendes blockiert wird:

- Unangemessene Webseiten.
- Den Internetzugang zu bestimmten Zeiten (beispielsweise während der Schule).
- Web-Seiten, Mails und Sofortnachrichten mit bestimmten Schlüsselwörtern.
- Anwendungen wie Spiele, Chat, Filesharing-Programme oder Andere.
- Sofortnachrichten, die von nicht erlaubten IM-Kontakten gesendet werden.



Wichtig

Nur Benutzer mit administrativen Rechten (Systemladministratoren) können auf die Kindersicherung zugreifen und sie konfigurieren. Um sicherzustellen, dass nur Sie die Einstellungen der Kindersicherung für alle Benutzer ändern können, sichern Sie sie mit einem Passwort. Sie werden dazu aufgefordert, das Passwort zu konfigurieren, wenn Sie die Kindersicherung für einen bestimten Benutzer aktivieren.

Um die Kindersicherung erfolgreich zu verwenden, um die Online- und Computeraktivität Ihrer Kinder zu begrenzen, müssen Sie diese wichtigsten Aufgaben fertigstellen:

1. Erstellen Sie begrenzte (standard) Windows-Benutzerkonten für Ihre Kinder.

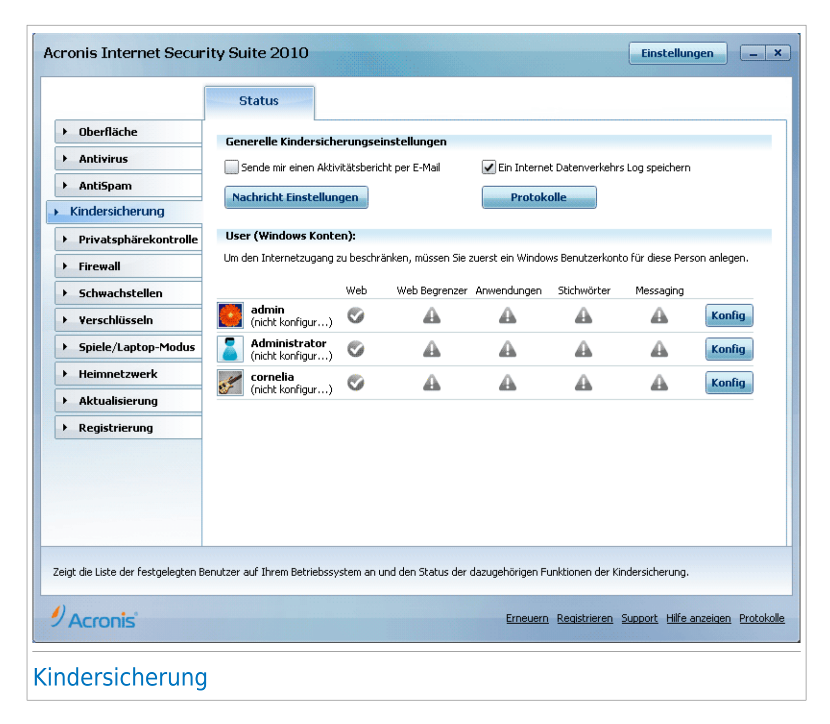


Anmerkung

Um herauszufinden wie Sie Windows-Benutzerkonten erstellen können, öffnen Sie die Windows Hilfe/Support (Klicken Sie im Startmenu auf **Hilfe und Support**).

2. Konfigurieren Sie die Kindersicherung für die Windows-Benutzerkonten Ihrer Kinder.

Um die Kindersicherung zu konfigurieren gehen Sie zu **Kindersicherung** in der erweiterten Ansicht.



Kindersicherung

Sie können Informationen bezüglich der Kindersicherung für jeden Windwos Benutzerkonto ansehen. Die Alterskategorie erscheint unterhalb jedes Benutzernamens wenn die Kindersicherung aktiviert ist. Wenn man die Kindersicherung deaktiviert, ist der Status **nicht konfiguriert**.

Zusätzlich können Sie den Status der Kindersicherung für jeden Benutzer sehen:

Grüner Kreis mit einem Häkchen: Die Einstellung ist aktiviert.
Roter Kreis mit einem Ausrufezeichen: Die Einstellung ist deativiert.

Klicken Sie die **Ändern** -Schaltfläche neben einem Benutzernamen um das Fenster zum Einstellen der Kindersicherung für das entsprechende Benutzerkonto zu öffnen.

Die folgenden Abschnitte in diesem Kapitel beschreiben detailliert die Funktionen der Kindersicherung und wie Sie sie verwenden können.

19.1. Kindersicherung für einen Benutzer konfigurieren.

Um die Kindersicherung für ein bestimmtes Benutzerkonto zu aktivieren, klicken Sie die Schaltfläche **Anpassen** neben dem entsprechenden Konto und wechseln Sie dann auf die **Status** Seite.



Status der Kindersicherung

Um die Kindersicherung für dieses Benutzerkonto zu konfigurieren, befolgen Sie die folgenden Schritte:

1. Aktivieren Sie die Kindersicherung für dieses Benutzerkonto, indem Sie das Kontrollkästchen neben **Kindersicherung** markieren.



Wichtig

Lassen Sie die **Kindersicherung** aktiviert, um Ihre Kinder gegen Jugendgefährdende Internet Inhalte zu schützen. Nutzen Sie dabei Ihre selbst festgelegten Regeln.

2. Stellen Sie ein Passwort ein, um Ihre Einstellungen für die Kindersicherung zu schützen. Für weitereInformationen besuchen Sie bitte *„Kindersicherung Einstellungen“* (S. 176).
3. Stellen Sie die Alterkategorie so ein Ihrem Kind den Zugriff auf Webseiten nur seinem Alter gemäß zu gestatten. Für weitere Informationen besuchen Sie bitte *„Alterskategorie einstellen“* (S. 177).
4. Konfigurieren Sie die Überwachungsfunktion für diesen Benutzer wie benötigt:

- **Einen Aktivitätsbericht an mich, über die E-Mail senden.** Eine E-Mail Benachrichtigung wird versendet, sobald die Kindersicherung eine Aktivität dieses Nutzers blockiert hat.
- **Speichere einen Internetverkehrbericht ab.** Speichert die von einem Benutzer besuchten Webseiten in einem Bericht.

Weitere Informationen erhalten Sie unter *„Kinderaktivität überwachen“* (S. 180).

5. Klicken Sie ein Icon oder Tab um die entsprechenden Kindersicherungsfunktionen festzulegen:
   - **Web-Kontrolle** - um die Web-Navigation gemäß der von Ihnen festgelegten Regeln in dem Bereich Web zu filtern.
   - **Programm-Kontrolle** - blockiert den Zugang zu Programmen, die Sie in dem Abschnitt Programme festgelegt haben.
   - **Stichwort-Filter** - um den Web-, Mail- und Instant Messaging-Zugriff nach den Regeln zu filtern, die Sie im Abschnitt Stichwörter festgelegt haben.
   - **Instant Messaging-Kontrolle** - um den Chat mit IM-Kontakten, entsprechend der von Ihnen im Abschnitt IM-Datenverkehr festgelegten Regeln zu erlauben oder zu verweigern.
   - **Webzeitbegrenzung** - um den Zugang zum Internet zeitlich einzugrenzen, wie Sie es im Abschnitt Zeitbegrenzung festgelegt haben.



Anmerkung
Um zu lernen wie Sie diese konfigurieren können, beachten Sie bitte die folgenden Inhalte in diesem Kapitel.

Um jeden Zugriff auf das Internet zu unterbinden, klicken Sie den Button **Internet blockieren**.

19.1.1. Kindersicherung Einstellungen

Wenn Sie nicht der einzige Benutzer des Computers mit administrativen Rechten sind, empfehlen wir Ihnen, Ihre vorgenommenen Einstellungen der Kindersicherung mit einem Passwort zu schützen. Wenn Sie ein Passwort einstellen, können andere Benutzer mit administrativen Rechten die Einstellungen der Kindersicherung nicht verändern.

Acronis Internet Security Suite 2010 wird Sie nach der Einstellung eines Passwortes fragen, wenn Sie die Kindersicherung aktivieren.



BitDefender per Passwort schützen

Um den Passwortschutz einzustellen, befolgen Sie die folgenden Schritte:

1. Geben Sie das Passwort in das Feld **Passwort** ein.
2. Geben Sie das Passwort erneut in das Feld **Passwort wiederholen** ein, um es zu bestätigen.
3. Klicken Sie auf **OK**, um das Passwort zu speichern und das Fenster zu schließen.

Von nun an werden Sie stets aufgefordert, Ihr Passwort einzugeben, wenn Sie die Einstellungen der Kindersicherung ändern wollen. Andere Systemadministratoren (falls vorhanden) müssen dieses Passwort ebenfalls angeben um Einstellungen der Kindersicherung zu ändern.



Anmerkung

Dieses Passwort wird nicht die anderen Einstellungen von Acronis Internet Security Suite 2010 schützen.

Wenn Sie kein Passwort einstellen, und nicht möchten, dass dieses Fenster erneut erscheint, aktivieren Sie **Nicht nach Passwort fragen wenn die Kindersicherung aktiviert wird**.

19.1.2. Alterskategorie einstellen

Der Heuristische Web Filter analysiert Webseiten und blockiert solche welche einen potenziel unangebrachten Inhalt enthalten.

Stellen Sie eine bestimmte Toleranzstufe ein, um den Internetzugang entsprechend vordefinierten altersbasierenden Regeln zu filtern. Ziehen Sie den Zeiger an der

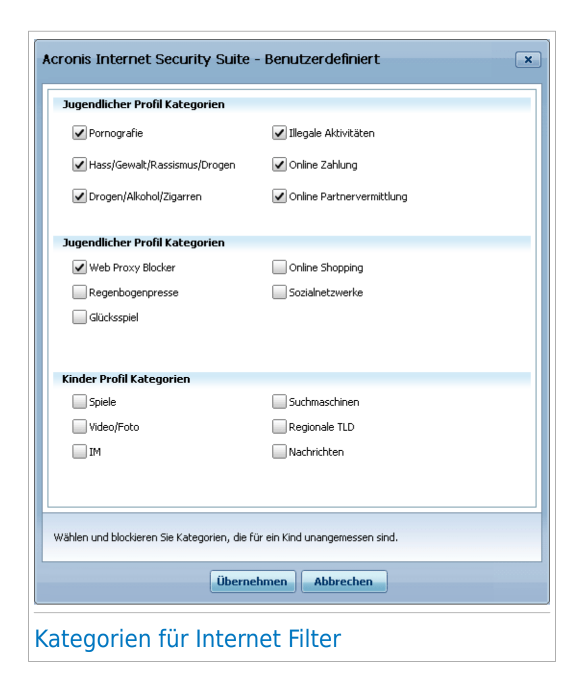
Scala entlang um die Stufe für den gewünschten Schutz einzustellen, den Sie für den Anwender für angemessen halten.

Es stehen 3 Toleranzstufen zur Verfügung:

Toleranzeinstellung	Beschreibung
Kind	Bietet eingeschränkten Zugriff auf das Internet, gemäß den Empfehlungen für Anwender unter 14 Jahren. Internet Seiten mit möglicherweise schädlichen Inhalten für Kinder (Porno Seiten, Sex Seiten etc.) werden blockiert.
Jugendlicher	Bietet eingeschränkten Zugriff auf das Internet, gemäß den Empfehlungen für Anwender von 14 bis 18 Jahren. Internet Seiten mit sexuellen oder pornographischen Inhalten werden blockiert.
Erwachsen	Bietet uneingeschränkten Zugang zum Internet unabhängig von den Inhalten der Internetseiten.

Klicken Sie auf **Standard**, um den Zeiger auf die Standard Einstellung zu ziehen.

Wenn Sie mehr Kontrolle über die Inhalte benötigen, die den Nutzern im Internet angezeigt werden, können Sie die verschiedenen Inhaltskategorien wählen die blockiert werden sollen. Um auszuwählen welche Web-Inhalte blockiert werden, klicken Sie **Angepasste Kategorien**. Ein neues Fenster wird sich öffnen:



Kategorien für Internet Filter

Markieren Sie das zugehörige Kästchen der Kategorie, die sie blockieren wollen und der Benutzer wird keinen Zugriff auf Websieten erhalten, die der Kategorie entsprechen. Um Ihnen die Auswahl zu erleichtern, sind die Kategorien der Web-Inhalte nach Altersgruppen sortiert.

- Die **Kinder** Profil-Kategorien enthalten Inhalte, die für Kinder unter 14 Jahren geeignet sind.

Kategorie	Beschreibung
Spiele	Webseiten die Browser-Spiele, Spiele-Foren, Spiele-Downloads, Cheats, Infos, etc. anbieten
Video/Foto	Webseiten die Video- oder Fotogalerien beinhalten.
IM	Instant Messaging Anwendungen.
Suchmaschinen	Such-Maschinen und -Portale.
Örtliche TLD	Webseiten die einen Domain auserhalb Ihrer Region haben.
Nachrichten	Online-Zeitungen.

- **Profil Kategorien für Jugendliche** Inhalte die für Kinder zwischen 14 und 18 Jahren als unbedenklich eingestuft werden.

Kategorie	Beschreibung
Web Proxy Blocker	Webseiten die verwendet werden um die URL einer angeforderten Seite zu maskieren.
Tabloids	Online Magazine.
Glücksspiele	Online Casinos, Wett-Webseiten, Webseiten die Wett-tipps anbieten, Wett-Forum, etc.
Online Shopping	Online Shops und Warenhäuser.
"Social Networks"	Social Network Webseiten.

- Die **Erwachsenen** Profil-Kategorien enthalten Inhalte, die für Kinder und Jugendliche nicht geeignet sind.

Kategorie	Beschreibung
Pornografie	Webseiten mit pornografischen Inhalten.
Hass/ Gewalt/ Rassismus/ Drogen	Webseiten die Gewalt, Rassismus, Terrorismus oder Drogen verherrlichen.
Drogen / Spirituosen / Zigarren	Webseiten die Drogen, Alkohol oder Tabakprodukte anpreisen oder verkaufen.
Illegale Aktivitäten	Webseiten die Raubkopien unterstützen oder Raubkopien zur verfügung stellen.
Online Bezahlung	Web-Formulare für Online-Bezahlung und Kassenbereiche von Online-Geschäften. Der Benutzer kann Online-Geschäfte besuchen, Kaufversuche werden jedoch blockiert.
Online Dating	Online Partnersuche mit Chat, Video oder Photo-Austausch.

Klick **Zuweisen** um die Kategorien der für den Benutzer zu sperrenden Webinhalte zu speichern.

19.2. Kinderaktivität überwachen

Acronis Internet Security Suite 2010 hilft Ihnen dabei festzustellen, was Ihre Kinder am Computer tun, auch wenn Sie nicht da sind. Sie können sich per E-Mail benachrichtigen lassen wann immer das Kindersicherungsmodul Aktivitäten blockiert. Zusätzlich können Sie ein Protokoll der vergangenen Aktivitäten speichern.

Wählen Sie die zu aktivierenden Optionen aus:

- **Einen Aktivitätsbericht an mich, über die E-Mail senden.** Eine E-Mail Benachrichtigung wird versendet, sobald die Kindersicherung eine Aktivität dieses Nutzers blockiert hat.
- **Speichere einen Internetverkehrbericht ab.** Zeichnet die besuchten Webseiten auf für Benutzer welche der Kindersicherung unterliegen.

19.2.1. Besuchte Webseiten überprüfen

Acronis Internet Security Suite 2010 zeichnet standardmässig die von Ihren Kindern besuchten Webseiten auf.

Um die Aufzeichnungen einzusehen, klicken Sie **Protokolle** um Historie&Ereignisse zu öffnen und wählen Sie **Internet Aufzeichnungen**.

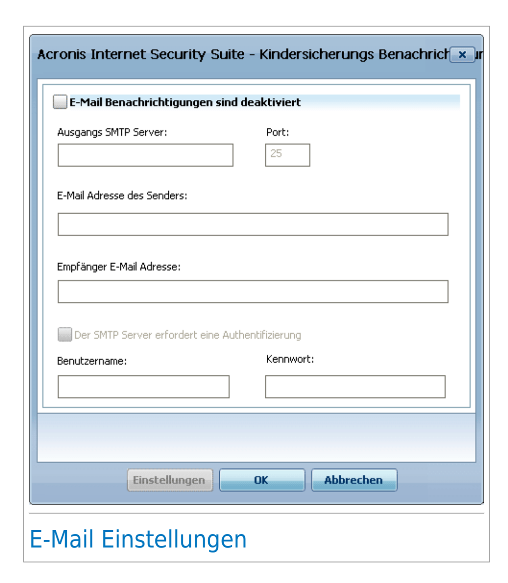
19.2.2. E-Mail-Benachrichtigungen konfigurieren

Um E-Mail Benachrichtigungen zu erhalten wenn die Kindersicherung eine Aktivität blockiert, wählen Sie **Aktivitätsbericht per E-Mail senden** im allgemeinen Konfigurationsfenster der Kindersicherung. Sie werden aufgefordert die E-Mail-Kontoeinstellungen zu konfigurieren. Klicken Sie **Ja** um das Konfigurationsfenster zu öffnen.



Anmerkung

Sie können das Konfigurationsfenster später öffnen indem Sie **Benachrichtigungseinstellungen** klicken.



E-Mail Einstellungen

Sie müssen die E-Mail-Kontoeinstellungen wie folgt konfigurieren:

- **Ausgehnder SMTP Server** - geben Sie die Adresse des Mail Servers, der für das Verschicken der E-Mails zuständig ist, ein.
- Falls der Server einen anderen als den Standardport 25 nutzt, geben Sie diesen bitte im entsprechenden Feld an.
- **Sender E-Mail Adresse** - geben Sie die Adresse ein die im **Von** Feld, der E-Mail, erscheinen soll.
- **Empfänger's E-Mail Adresse** - geben Sie die Adresse ein, an welche die Berichte gesandt werden sollen.
- Falls der Server Authentifikation verlangt, wählen Sie **Mein SMTP Server erfordert Authentifikation** aus und geben den Benutzernamen und das Passwort in die dazugehörigen Felder ein.



Anmerkung

Falls Ihnen die Einstellungen unbekannt sind, öffnen Sie den E-Mail Client und überprüfen Sie Ihre E-Mail Kontoeinstellungen.

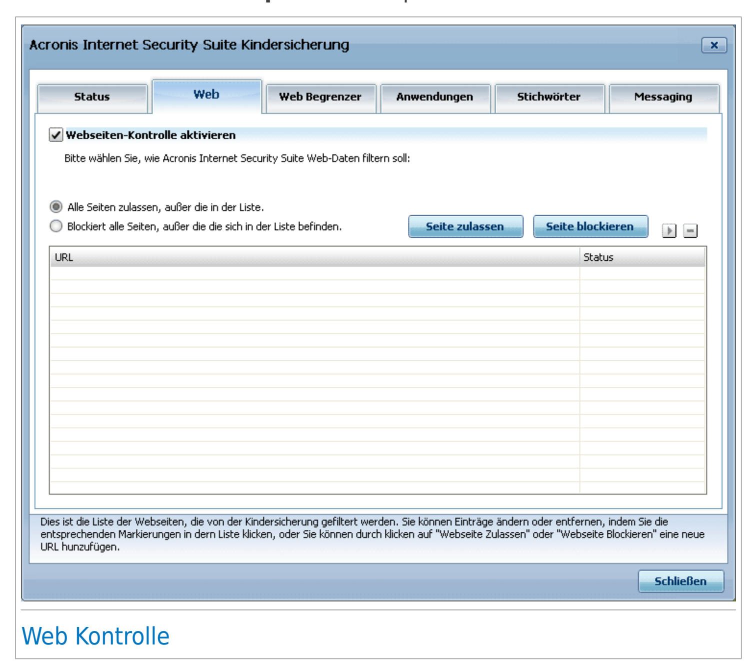
Um die Konfiguration zu bestätigen, klicken Sie **Einstellungen testen**. Falls während des Vorgangs Probleme auftauchen, wird Acronis Internet Security Suite 2010 Sie über die Bereiche, die Ihre Aufmerksamkeit erfordern, informieren.

Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

19.3. Web Kontrolle

Die **Web-Seiten-Kontrolle** ermöglicht Ihnen, Web-Seiten mit fragwürdigem Inhalt zu sperren. Eine Liste geblockter Webseiten und Teilbereichen ist Ihnen bereits zur Verfügung gestellt und im Verlauf des normalen Update-Prozesses konstant erneuert.

Um die Web-Kontrolle für ein bestimmtes Benutzerkonto zu konfigurieren, klicken Sie die Schaltfläche **Anpassen** entsprechend dem Konto und klicken das **Web** Tab.



Web Kontrolle

Um diesen Schutz zu aktivieren wählen Sie entsprechend **Web-Kontrolle aktivieren** aus.

19.3.1. Web-Kontroll Regel erstellen

Um den Zugriff auf eine Webseite zu blockieren oder zu erlauben, folgen Sie diesen Schritten:

1. Klicken Sie **Seite erlauben** oder **Seite blockieren**. Ein neues Fenster erscheint:



Webseite festlegen

2. Geben Sie die Webseiten Adresse in das **Webseite** Feld ein.
3. Wählen Sie die gewünschte Aktion für diese Regel aus - **Erlauben** oder **Blocken**.
4. Klicken Sie auf **Beenden** um die Regel hinzuzufügen.

19.3.2. Web-Kontroll Regeln verwalten

Die bereits konfigurierten Webseitenkontrollregeln sind in der Tabelle am unteren Rand des Fensters aufgelistet. Die Adresse und der aktulle Status jeder Webkontroll-Regel sind aufgelistet.

Um eine Regel zu bearbeiten wählen Sie diese aus und klicken **Bearbeiten** und führen die erforderlichen Änderungen im Konfigurationsfenster durch. Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche.

Legen Sie zudem fest welche Aktion die Acronis Internet Security Suite 2010 Kindersicherung für Web-Seiten vornehmen soll für die keine Web-Kontroll Regeln existieren:

- **Alle Seiten ausser die der Liste erlauben**. Wählen Sie diese Option um den Zugriff auf alle Webseiten, ausser auf solche die Sie auf **Blockieren** gesetzt haben, zu erlauben.
- **Alle Seiten ausser die der Liste blockieren**. Wählen Sie diese Option um den Zugriff auf alle Webseiten, ausser auf solche die Sie auf **Erlauben** gesetzt haben, zu blocken.

19.4. Zeitplan

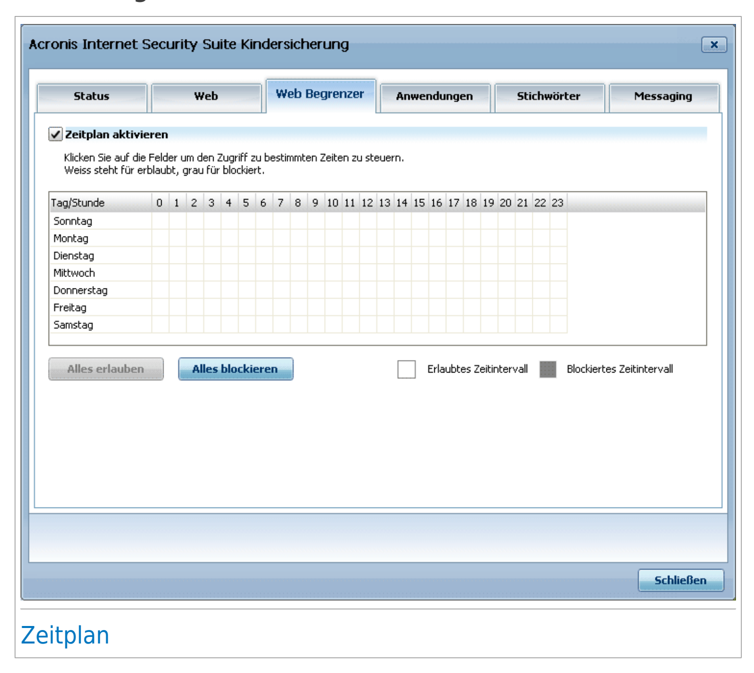
Dieser **Zeitplan** erlaubt Ihnen, den Zugriff zum Internet über Personen oder Programme zeitlich zu bestimmten.



Anmerkung

Acronis Internet Security Suite 2010 wird Aktualisierungen jede Stunde unabhängig von der Einstellungen vom **Webzeitbegrenzer** durchführen.

Um den Online-Zeitbegrenzer für einen bestimmten Benutzer zu konfigurieren, klicken Sie **Anpassen** für das dazugehörige Benutzerkonto und klicken auf das **Online-Begrenzer**-Tab.



Zeitplan

Um diese Schutzfunktion zu aktivieren, setzen Sie bitte das entsprechende Häkchen in der Häkchenbox analog zu **Zeitplan aktivieren**.

Wählen Sie die gewünschten Zeitintervalle wo alle Internetverbindungen blockiert werden. Sie können einzelne Zellen anklicken oder ganze Spalten markieren. Ausserdem können Sie **Alles markieren** klicken um alle Zellen auszuwählen und die Anwendung komplett zu blockieren. Wenn Sie **Alles unmarkiert** klicken, wird der Zugriff auf die Anwendung jederzeit erlaubt.



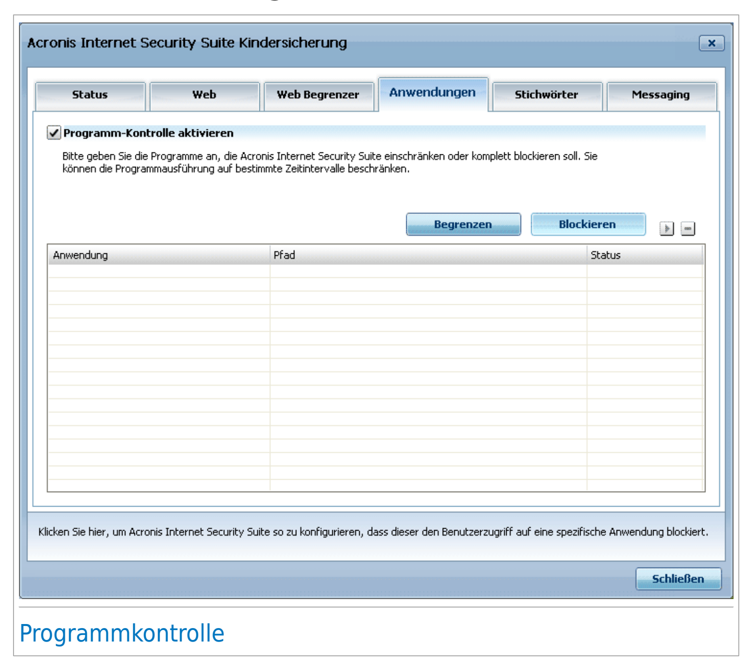
Wichtig

Die grau markierten Fenster entsprechen den Zeitintervallen, in denen alle Internetaktivitäten gesperrt sind.

19.5. Programmkontrolle

Die **Programm-Kontrolle** unterstützt Sie bei der Sperrung jeglicher Programmanwendungen. Spiele, Medien- und Messaging Software als auch andere Kategorien von Programmen oder gefährlicher Software können auf diesem Wege blockiert werden. Programme, die über diesen Weg gesperrt sind, können weder verändert, kopiert noch verschoben werden. Sie können Anwendungen permanent blocken oder nur für bestimmte Zeitintervalle, wie solche in denen Ihre Kinder Hausaufgaben zu erledigen haben.

Um die Anwenundungskontrolle für ein bestimmtes Benutzerkonto zu aktivieren, klicken Sie die Schaltfläche **Anpassen** neben dem entsprechenden Konto und klicken das **Anwendungen** Tab.



Programmkontrolle

Um diesen Schutz zu aktivieren wählen Sie entsprechend **Anwendungskontrolle aktivieren** aus.

19.5.1. Anwendungskontrollregeln erstellen

Um den Zugriff auf eine Anwendung zu beschränken oder zu blockieren, befolgen Sie diese Schritte:

1. Klicken Sie **Anwendung blockieren** oder **Anwendung einschränken**. Es erscheint ein neues Fenster:



Anwendung festlegen

2. Klicken Sie **Durchsuchen** um die Anwendung, für die Sie den Zugriff blockieren/einschränken wollen, herauszusuchen.
3. Wählen Sie die Aktion der Regel:
   - **Dauerhaft blockieren** um den Zugriff auf die Anwendung vollständig zu blockieren.
   - **Blockieren basierend auf dieser Planung** um den Zugriff für bestimmte Zeitintervalle einzuschränken.

   Wenn Sie sich entscheiden den Zugriff einzuschränken statt die Anwendung komplett zu blockieren, so müssen Sie im Planungsgitter die Tage und das Zeitintervall auswählen währenddessen der Zugriff blockiert ist. Sie können einzelne Zellen durch Klicken anwählen oder die Maustaste gedrückt halten um Bereiche zu wählen. Außerdem können Sie **Alle auswählen** und damit die Anwendung komplett blockieren. Wenn Sie **Alle abwählen** klicken, wird der Zugriff auf die Anwendung zu jeder Zeit gestattet.

4. Klicken Sie auf **Beenden** um die Regel hinzuzufügen.

19.5.2. Anwendungs-Kontrolle Regeln verwalten.

Die bereits erstellten Anwenungskontrollregeln werden in der Tabelle am unteren Ende des Fensters aufgelistet. Es wird für jede Regel der Name der Anwendung, der Pfad und der aktuelle Status aufgelistet.

Um eine Regel zu bearbeiten wählen Sie diese aus und klicken **Bearbeiten** und führen die erforderlichen Änderungen im Konfigurationsfenster durch. Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche.

19.6. Schlüsselwortkontrolle

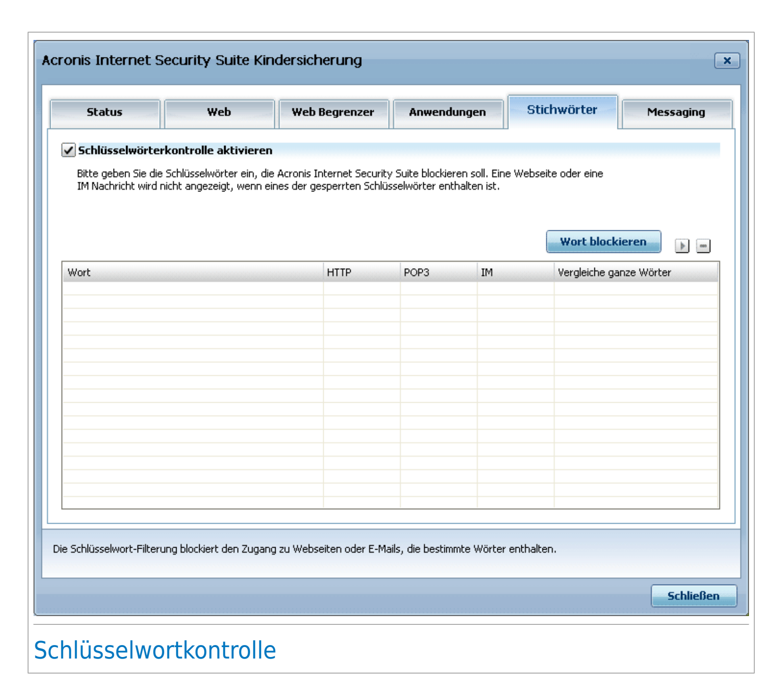
Mit der Schlüsselwortfilterung können Sie den Zugang zu E-Mail Nachrichten, Webseiten und Sofortnachrichten, die bestimmte Wörter enthalten, blockieren. Mit der Schlüsselwortfilterung können Sie verhindern, dass Ihre Kinder unangemessene Wörter oder Sätze sehen, wenn sie online sind.



Anmerkung

Die Schlüsselwortfilterung für Instant Messaging ist nur für Yahoo Messenger und Windows Live (MSN) Messenger verfügbar.

Um die Schlüsselwortfilterung für ein bestimmtes Benutzerkonto zu konfigurieren, klicken Sie die Schaltfläche **Ändern** entsprechend dem Konto und klicken das **Schlüsselworter** Tab



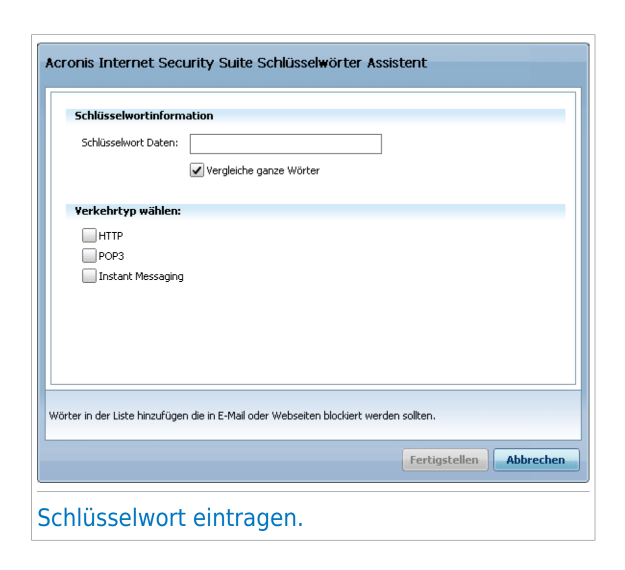
Schlüsselwortkontrolle

Markieren Sie das Kontrollkästchen **Schlüsselwortfilterung aktivieren**, wenn Sie diese Funktion verwenden wollen.

19.6.1. Erstellen von Regeln für die Schlüsselwortfilterung

Um ein Wort oder eine Phrase zu blockieren folgen Sie diesen Schritten:

1. Klicken Sie **Schlüsselworte blockieren**. Es öffnet sich ein neues Fenster.



Schlüsselwort eintragen.

2. Geben Sie das Wort oder den Satz den Sie blockieren möchten in das Eingabefeld ein. Wenn nur ganze Wörter erkannt werden sollen wählen Sie die Option **Nur ganze Wörter suchen**.
3. Wählen Sie den Datenverkehrs-Typ, den Acronis Internet Security Suite 2010 nach den definierten Worten prüfen soll.

Optionen	Beschreibung
HTTP	Internet Seiten, die Schlüsselwörter enthalten, werden geblockt.
POP3	E-Mail Nachrichten, die das Schlüsselwort enthalten werden blockiert.
Instant Messaging	Sofortnachrichten, die das Schlüsselwort enthalten werden blockiert.

4. Klicken Sie auf **Beenden** um die Regel hinzuzufügen.

19.6.2. Regeln für die Schlüsselwortfilterung verwalten

Unten werden Ihnen die Regeln zur Schlüsselwortkontrolle angezeigt. Für jede Regel werden zudem die Wörter und der gegenwärtige Status für die entsprechenden Netzwerkprotokolle angegeben.

Um eine Regel zu bearbeiten wählen Sie diese aus und klicken **Bearbeiten** und führen die erforderlichen Änderungen im Konfigurationsfenster durch. Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche.

19.7. Instant Messaging (IM) Kontrolle

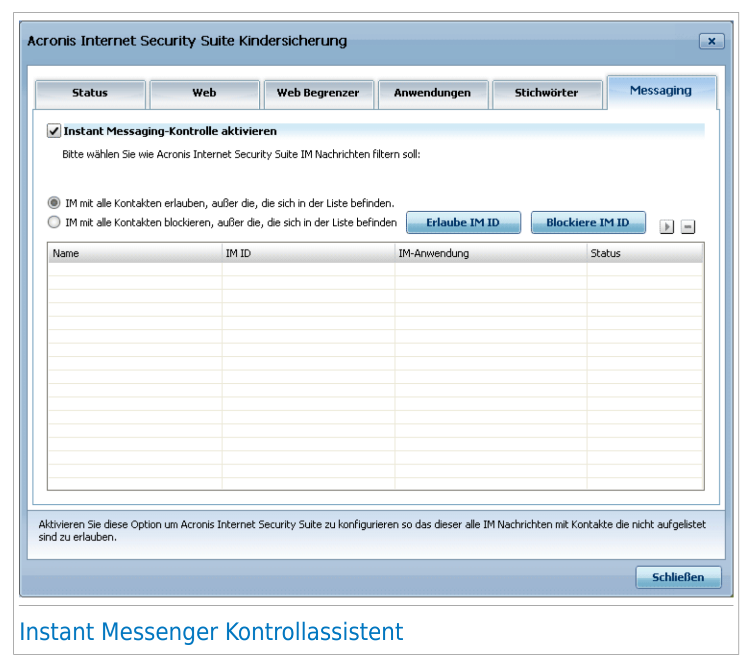
Die Instant Messaging (IM) Kontrolle gibt Ihnen die Möglichkeit IM-Kontakte festzulegen, mit denen Ihre Kinder chatten dürfen.



Anmerkung

Die IM-Kontrolle ist nur für Yahoo Messenger und Windows Live (MSN) Messenger verfügbar.

Um die IM-kontrolle für ein bestimmtes Benutzerkonto zu aktivieren, klicken Sie **Anpassen** neben dem entsprechenden Konto und klicken das **Messenger** Tab.



Instant Messenger Kontrollassistent

Markieren Sie das Kontrollkästchen **Instant Messaging Kontrolle aktivieren** wenn Sie diese Kontrollfunktion verwenden möchten.

19.7.1. Erstellen von Instant Messaging (IM)Kontroll-Regenl

Um IM-Konversationen mit einem Kontakt zu erlauben oder zu blockieren, folgen Sie diesen Schritten:

1. Klicken Sie **IM ID blockieren** oder **IM ID erlauben**. Es erscheint ein neues Fenster:



Fügen Sie einen IM-Kontakt hinzu

2. Geben Sie den Name der Kontaktperson in das **Name** -Feld ein.
3. Geben Sie die E-Mail Adresse oder den Nutzernamen, der von dem IM Kontakt genutzt wird, in das Feld **E-Mail oder IM ID** ein.
4. Wählen Sie das Chatprogramm das der Kontakt verwendet.
5. Wählen Sie die gewünschte Aktion für diese Regel aus - **Blocken** oder **Erlauben**
6. Klicken Sie auf **Beenden** um die Regel hinzuzufügen.

19.7.2. Erstellen von Instant Messaging (IM)Kontroll-Regeln

Die IM Kontrollregeln, die konfiguriert wurden, sind in einer Tabelle in der unteren Hälfte des Fensters aufgelistet. Der Name, die IM ID, IM Anwendung und der aktulle Status jeder IM Kontroll-Regel sind aufgelistet.

Um eine Regel zu bearbeiten wählen Sie diese aus und klicken **Bearbeiten** und führen die erforderlichen Änderungen im Konfigurationsfenster durch. Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche.

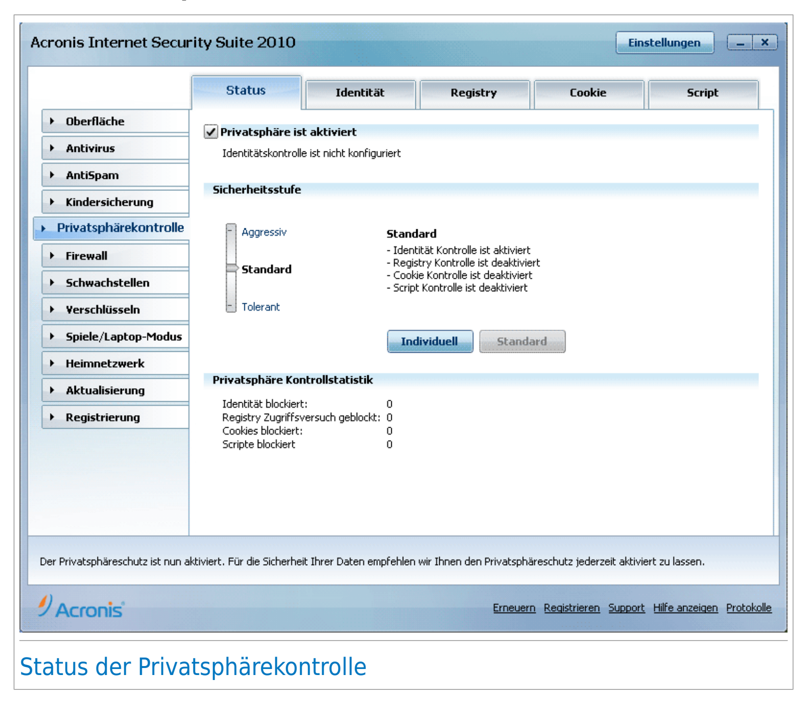
Sie sollten des weiteren festlegen welche Aktion die Kindersicherung für IM-Kontakte vornehmen soll für welche keine Regel erstellt wurde. Wählen Sie **Blockieren** oder **IM-Konversationen mit allen Kontakten ausser denen der Liste erlauben**.

20. Privatsphärekontrolle

Acronis Internet Security Suite 2010 überwacht dutzende von möglichen Angriffspunkten (sog. "HotSpots") in Ihrem System, die durch Spyware befallen werden könnten. Es überprüft ebenfalls jede Veränderung innerhalb des Systems und der vorhandenen Software. Bekannte Spyware-Programme werden in Echtzeit blockiert. Acronis Internet Security Suite 2010 ist höchst effizient in der Bekämpfung von Trojanischen Pferden oder auch anderen bösartigen Instrumenten von Crackern (oftmals als Hacker bezeichnet). Sie bietet einen zuverlässigen Schutz vor Angriffen auf Ihre Privatsphäre und dem unbefugten Versenden persönlicher Daten wie z.B. Kreditkartennummern, PINs oder TANs, usw. von Ihrem Computer zum Angreifer.

20.1. Status der Privatsphärekontrolle

Um die Privatsphäre zu konfigurieren und Informationen dazu zu erhalten klicken Sie auf **Privatsphäre>Status** in der Profiansicht.



Status der Privatsphärekontrolle

Sie können ob die Privatssphäre aktiviert ist oder nicht. Wenn Sie den Status der Privatssphäre ändern möchten, markieren Sie die entsprechende Option, oder lassen Sie sie frei.



Wichtig
Um Datendiebstahl vorzubeugen und private Daten zu schützen, lassen Sie die **Privatsphäre** aktiviert.

Die Privatsphäre schützt Ihren Computer mit diesen wichtigen Kontrollmechanismen:

- Identitätskontrolle - schützt Ihre vertrauenswürdigen Daten indem der gesamte ausgehende HTTP- und SMTP- (Web/E-Mail) sowie der Instant Messaging-Datenverkehr gemäß den Regeln, die Sie in dem Abschnitt Identität festgelegt haben, gefiltert wird.
- Registry-Kontrolle - fragt um Erlaubnis immer wenn ein Programm versucht die Registry zu ändern um beim Windows Neustart ausgeführt zu werden.
- Cookie-Kontrolle- fragt nach Ihrer Einwilligung, sobald eine neue Webseite einen Cookie auf Ihrem Rechner installieren will.
- Skript-Kontrolle- fragt nach Ihrer Einwilligung, sobald eine Webseite versucht, ein Skript oder andere aktive Inhalte zu aktivieren.

Im unteren Bereich können Sie die **Privatsphäre Statistiken** einsehen.

20.1.1. Sicherheitsstufe einstellen

Sie können die Sicherheitseinstellung an Ihre Anforderungen anpassen. Ziehen Sie die Anzeige auf der Scala auf die richtige Einstellung.

Es gibt 3 mögliche Einstellungen:

Sicherheitseinstellung	Beschreibung
Tolerant	Alle Schutzkontrollen sind deaktiviert.
Standard	Nur **Identitätskontrolle** ist aktiviert.
Aggressiv	**Identitätskontrolle**, **Registrykontrolle**, **Cookie-Kontrolle** und **Script-Kontrolle** sind aktiviert.

Sie können die Sicherheitsstufe für den gewünschten Schutz einstellen. Klicken Sie hierfür auf**Stufe anpassen**. Wählen Sie in dem Fenster das sich öffnet die gewünschten Sicherheitsstufen und klicken Sie auf **OK**.

Mit dem Klick auf **Standard** laden Sie die Grundeinstellungen.

20.2. Antispyware/Identitätskontrolle

Vertrauliche Daten zu sichern ist für alle Anwender äußerst wichtig. Datenklau hat mit der Entwicklung der Internet Kommunikation standgehalten und wendet immer wieder neue Methoden an um Anwender zu täuschen und private Informationen zu erhalten.

Ob es sich um Ihre E-Mail Adresse handelt oder um Ihre Kreditkartennummer, wenn sie in die falschen Hände geraten können diese Informationen großen Schaden anrichten: Sie werden möglicherweise in Spam Mails ertrinken oder sich über ein geleertes Konto wundern.

Die Identitätskontrolle schützt Sie gegen den Diebstahl wichtiger Daten, wenn Sie online sind. Basierend auf Regeln, die von Ihnen erstellt wurden, prüft die Identitätskontrolle den Web-, Mail und IM-Datenverkehr auf spezielle Zeichenfolgen (zum Beispiel Ihre Kreditkartennummer). Wenn eine Übereinstimmung mit einer Webseite, E-Mail Adresse oder IM-Nachricht gefunden wird, werden diese sofort geblockt.

Sie können Regeln erstellen, um jegliche Information zu schützen, die Sie als persönlich oder vertraulich betrachten, von Ihrer Telefonnummer oder E-Mail-Adresse bis hin zu Ihren Bankkontoangaben. Es wird eine Multiuser Unterstützung zur Verfügung gestellt, wodurch Benutzer die sich in verschiedene Windows-Benutzerkonten einloggen Ihre eigenen Regeln zur Identitätskontrolle konfigurieren können. Falls Ihr Windows-Benutzerkonto ein Administratorkonto ist, können die von Ihnen erstellten Regeln festgelegt werden, auch zu gelten wenn andere Benutzer mit deren Konten am Windows eingeloggt sind.

Warum sollten Sie die Identitätskontrolle verwenden?

- Die Identitätskontrolle kann Keylogger-Spyware effektiv blockieren. Diese schädlichen Anwendungen speichern Ihre eingegebenen Tastenfolgen und senden sie über das Internet zu Hackern. Der Hacker kann über diese gestohlenen Daten sensible Informationen erfahren, so wie Kontonummern und Passwörter und kann Sie zu seinem eigenen Profit verwenden.

  Auch wenn eine solche Anwendung es schafft die Antivirus-Entdeckung zu umgehen, kann es die gestohlenen Daten nicht über E-Mail, das Internet oder Chatprogramme senden, wenn Sie entsprechende Regeln für die Identitätskontrolle eingestellt haben.

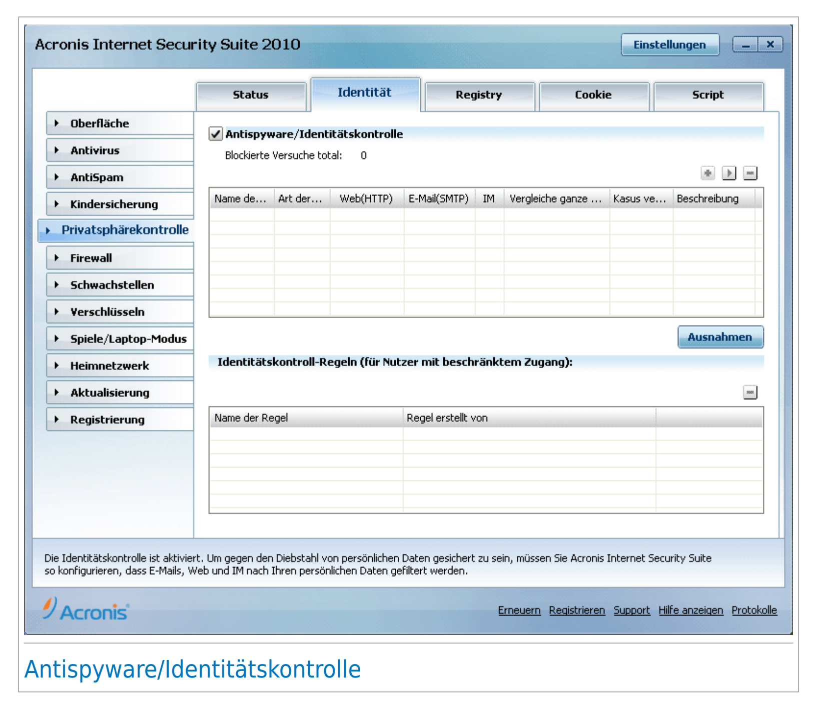
- Die Identitätskontrolle kann Sie vor Phishing schützen (Versuche, persönliche Daten zu stehlen). Die meisten Phishing-Versuche verwenden eine betrügerische E-Mail, um Sie dazu zu bringen persönliche Daten an eine gefälschte Webseite zu senden.

  So können Sie beispielsweise eine E-Mail erhalten, die behauptet von Ihrer Bank zu kommen und Sie dazu auffordert, Ihre Bankangaben dringend zu aktualisieren. In der E-Mail befindet sich ein Link zu einer Webseite, auf der Sie Ihre persönlichen Daten angeben sollen. Auch wenn dies alles echt erscheint, sind sowohl die E-Mail als auch die genannte Webseite Fälschungen. Wenn Sie auf den Link in der Mail klicken und Ihre persönlichen Daten an die Webseite senden, werden Sie diese Informationen an Hacker weiterleiten, die diesen Phishing-Versuch erstellt haben.

  Wenn entsprechende Regeln für die Identitätskontrolle eingestellt sind, können Sie die persönlichen Daten (so wie Ihre Kreditkartennummer) nicht an eine

Webseite senden, außer wenn Sie die entsprechende Seite explizit als Ausnahme festgelegt haben.

Um die Identitätskontrolle zu konfigurieren klicken Sie auf **Privatssphäre>Identität** in der Profiansicht.



Antispyware/Identitätskontrolle

Wenn Sie die Identitätskontrolle verwenden möchten, befolgen Sie folgende Schritte:

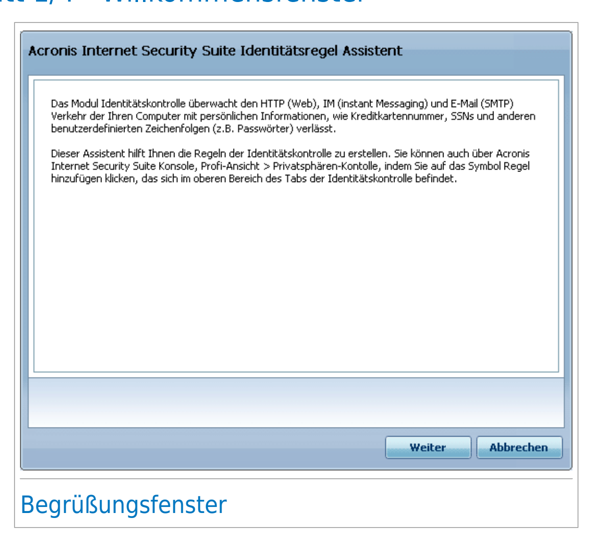
1. Wählen Sie **Identitätskontrolle aktivieren** aus.
2. Erstellen Sie Regeln um wichtige Daten zu schützen. Für weitere Informationen lesen Sie bitte *„Erstellen von Privatssphäreregeln"* (S. 198).
3. Wenn nötig, Erstellen Sie spezielle Ausnahmen zu den Regeln, die Sie erstellt haben. Für weitere Informationen lesen Sie bitte *„Definition von Ausnahmen"* (S. 201).
4. Wenn Sie Administrator auf diesn Rechner sind, können Sie sich von den erstellten Identitätsregeln anderer Administratoren ausschließen.

   Für weitere Informationen lesen Sie bitte *„Regel die von anderen Administratoren definiert wurden."* (S. 203).

20.2.1. Erstellen von Privatssphäreregeln

Um eine Regel für die Identitätskontrolle zu erstellen, klicken Sie auf die Schaltfläche **Hinzufügen** und befolgen Sie die Schritte des Konfigurationsassistenten.

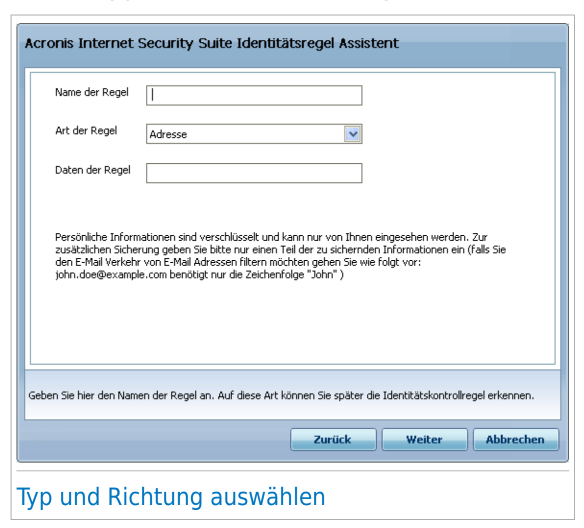
Schritt 1/4 - Willkommensfenster



Begrüßungsfenster

Klicken Sie auf **Weiter**.

Schritt 2/4 - Typ und Daten der Regel auswählen



Typ und Richtung auswählen

Hier können Sie die Parameter auswählen:

- **Name der Regel** - Geben Sie einen Namen für die Regel in dieses Editierfeld ein.
- **Art der Regel** - wählen Sie die Regel aus (Adresse, Name, Kreditkartennummer, PIN, TAN etc).
- Geben Sie in das Feld **Daten der Regel** die Daten ein, die geschützt werden sollen. Wenn Sie zum Beispiel Ihre Kreditkartennummer schützen wollen, geben Sie sie zum Teil oder ganz ein.



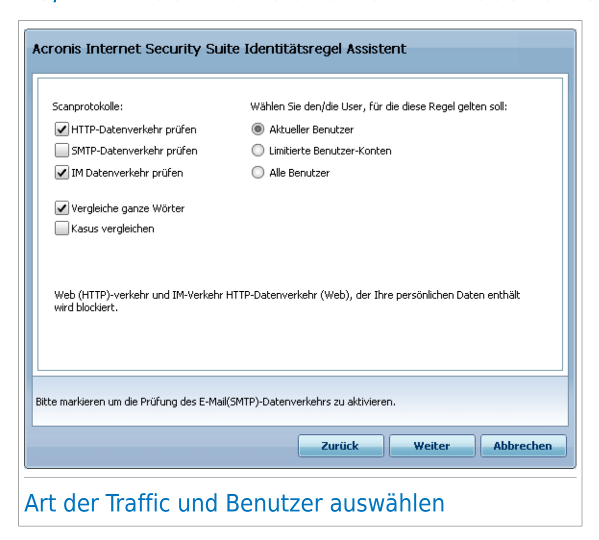
Anmerkung

Wenn Sie weniger als drei Zeichen angeben werden Sie aufgefordert die Daten zu überprüfen. Wir empfehlen die Eingabe von mindestens drei Zeichen um ein versehentliches blockieren von Nachrichten oder Webseiten zu verhindern.

Alle Daten, die Sie eingeben sind verschlüsselt. Um wirklich sicher zu gehen, geben Sie nicht alle Daten ein, die Sie schützen möchten.

Klicken Sie auf **Weiter**.

Schritt 3/4 - Art der Traffic und Benutzer auswählen



Art der Traffic und Benutzer auswählen

Bitte wählen sie den Datenverkehrstyp welchen Acronis Internet Security Suite 2010 prüfen soll. Die folgenden Optionen sind verfügbar:

- **HTTP-Daten überprüfen** - prüft den HTTP (web) Datenverkehr und blockiert ausgehende Daten, die den Regeln entsprechen.
- **SMTP-Daten überprüfen** - prüft alle ausgehenden E-Mail-Nachrichten, die den Regeln entsprechen.
- **Instant Messaging überprüfen** - prüft den Instant Messaging Datenverkehr und blockiert ausgehende Nachrichten, die den Regeln entsprechen.

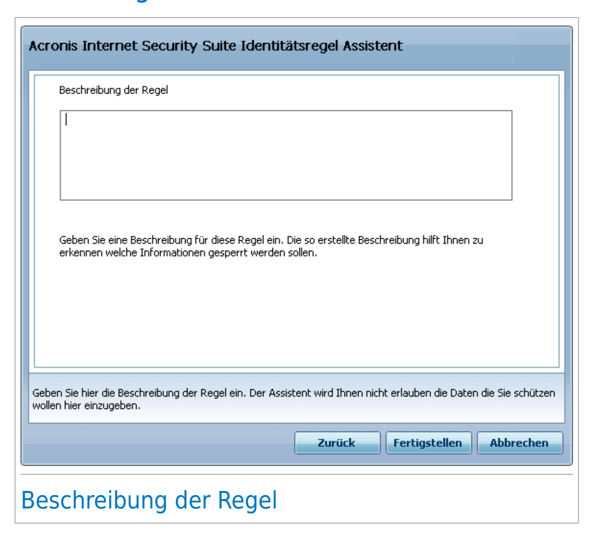
Sie können wählen ob die Regeln nur zutreffen, wenn die Daten der Regeln wörtlich übereinstimmen oder ob die komplette Zeichenfolge übereinstimmen muss.

Geben Sie den Benutzer an, für den die Regel angewendet werden soll.

- **Nur für mich(Aktueller Nutzer)** - Die Regel wird nur für Ihren Benutzerkonto angewendet.
- **Begrenzte Benutzerkonten** - Die Regel wird bei Ihren un alle anderen begrenzten Windows Benutzerkonten angewandt.
- **Alle Benutzer** - Die Regel wird an alle Windows-Benutzerkonten angewandt.

Klicken Sie auf **Weiter**.

Schritt 4/4 - Regel beschreiben



Beschreibung der Regel

Geben Sie eine kurze Beschreibung der Regel im Eingabefeld ein. Da die blockierten Daten (Zeichenfolgen) nicht als ein vollständiger Text angezeigt werden wenn auf die Regel zugegriffen wird, sollte Ihnen die Beschreibung dabei helfen sie einfach zu identifizieren.

Klicken Sie auf **Fertigstellen**. Die Regel wird in der Tabelle erscheinen.

20.2.2. Definition von Ausnahmen

In manchen Fällen wird es nötig sein Ausnahmen für bestimmte Identitätsregeln zu erstellen. Zum Beispiel haben Sie eine Regeln angelegt, welche verhindert das Ihre Kreditkartennummer per HTTP übertragen wird. Nun möchten Sie sich aber z.B. Schuhe auf einer bestimmten Webseite per Kreditkarte kaufen. In diesem Fall müssten Sie eine Ausnahme definieren um dies möglich zu machen.

Um eine solche Ausnahme zu erstellen klicken Sie auf die **Ausnahmen**-Schaltfläche.



Ausnahmen

Um eine Ausnahme zu erstellen befolgen Sie die folgenden Schritte:

1. Klicken Sie auf die Schaltfläche **Hinzufügen** um einen neuen Eintrag in die Tabelle hinzuzufügen.
2. Doppelklicken Sie auf **Entsprechende Ausschluss eingeben** und geben Sie die gewünschte URL, E-Mail Adresse oder IM-Kontakt ein, um sie Auszuschliessen.
3. Doppelklicken Sie dann auf **Typ wählen** und wählen Sie den gewünschten Eintrag aus dem Menü aus.
   - Wenn Sie eine Webseite eingegeben haben dann wählen Sie **HTTP**.
   - Wenn Sie eine E-Mail Adresse eingegeben haben dann wählen Sie **E-Mail (SMTP)**.
   - Wenn Sie einen IM-Kontakt eingegeben haben dann wählen Sie **IM**.

Um eine Ausnahme aus der Liste zu entfernen, wählen Sie diese aus und klicken auf die **Entfernen**-Schaltfläche.

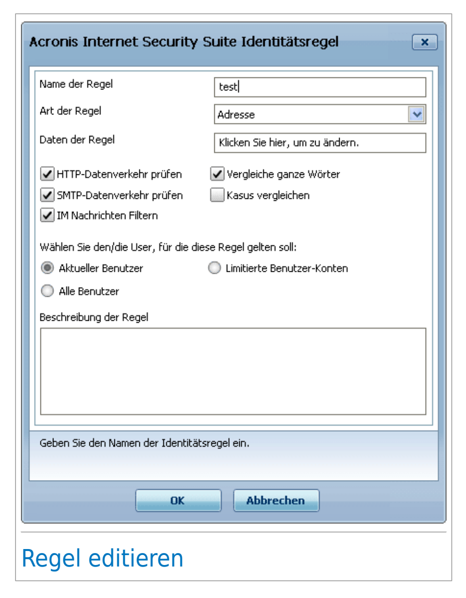
Klicken Sie auf **OK**, um die Änderungen zu speichern.

20.2.3. Regeln bearbeiten

Sie können eine Liste der Regeln in der Aufstellung ansehen.

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche.

Um eine Regel zu bearbeiten wählen Sie die Regel aus und klicken **Bearbeiten** oder machen Sie einen Doppelklick. Ein neues Fenster erscheint.



Regel editieren

Hier können Sie Namen, Beschreibungen und Parameter der Regel ändern. (Typ, Daten und Datenverkehr). Klicken Sie **OK** um die Änderungen zu speichern.

20.2.4. Regel die von anderen Administratoren definiert wurden.

Wenn Sie nicht der einzige Benutzer mit administrativen Rechte sind, können die anderen Administratoren eigene Identitätsregeln erstellen. Falls Sie die von anderen Benutzern erstellten Regeln nicht verwenden möchten wenn Sie eingeloggt sind, erlaubt es Ihnen Acronis Internet Security Suite 2010 sich von jeder Regel auszuschliessen die nicht von Ihnen erstellt wurde.

Sie können eine Liste mit der von anderen Administratoren erstellten Regeln in der Tabelle unter **Identitätskontrolle Regeln** Für jede Regel, wird der Name und der Benutzer der die Regel erstellt hat, angezeigt.

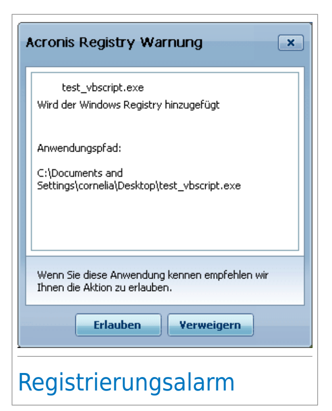
Um sich selbst von einer Regel auszuschliessen, wählen Sie die Regel aus der Tabelle aus und klicken die **Entfernen**-Schaltfläche.

20.3. Registrierung prüfen

Ein sehr wichtiger Teil von Windows ist die **Registry**. Dort werden von Windows alle Einstellungen, installierten Programme, Nutzerinformationen und so weiter verwaltet.

Die **Registry** bestimmt u. a., welche Programme automatisch beim Start von Windows geladen werden. Viren versuchen häufig hier anzusetzen, damit auch sie automatisch mit geladen werden, wenn der Nutzer seinen Computer startet.

Registry Kontrolle beobachtet die Windows-Registry – dies ist auch sehr hilfreich beim Aufspüren von Trojanern. Sie werden alarmiert, wann immer ein Programm versucht, einen Eintrag in die Registry zu unternehmen, um beim nächsten Windows-Start geladen zu werden.



Registrierungsalarm

Sie können das Programm sehen, das versucht die Windows-Registry zu modifizieren.

Wenn Sie das Programm nicht kennen und es Ihnen verdächtig erscheint, klicken Sie auf **Blockieren** um es davon abzuhalten die Windows-Registry zu verändern. Klicken Sie andererseits auf **Erlauben** um die Veränderung zu erlauben.

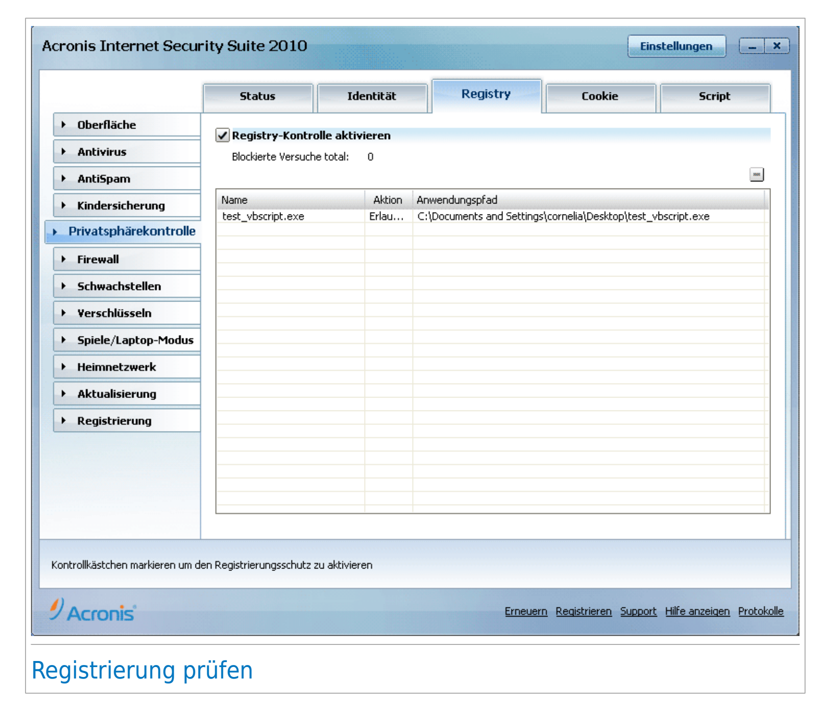
Je nach Ihrer Auswahl wird eine Regel erstellt und in der Regeltabelle aufgelistet. Dieselbe Aktion wird immer ausgeführt wenn diese Anwendung versucht einen Registryeintrag zu ändern.



Anmerkung

Acronis Internet Security Suite 2010 wird Sie bei der Installation neuer Programme informieren, wenn ein automatisches Starten nach der Windowsanmeldung erforderlich ist. In den meisten Fällen sind diese Programme legal und Sie können ihnen vertrauen.

Um die Identitätskontrolle zu konfigurieren klicken Sie auf **Privatssphäre>Identität** in der Profiansicht.



Registrierung prüfen

Sie können eine Liste der Regeln in der Aufstellung ansehen.

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die ⊟ **Löschen** Schaltfläche.

20.4. Cookie-Kontrolle

Cookies werden von den meisten Webseiten im Internet verwendet. Es sind kleine Dateien, die auf Ihrem Computer gespeichert werden. Webseiten verschicken diese Cookies, um das Surfen zu beschleunigen, aber auch um Informationen über Sie zu erhalten.

Generell erleichtern Cookies das tägliche Internet-Leben. Zum Beispiel ermöglichen sie einer Webseite, Ihren Namen und sonstige Angaben zu speichern, so dass Sie diese nicht bei jedem Besuch eingeben müssen.

Cookies können jedoch auch missbräuchlich verwendet werden und Ihre Privatsphäre gefährden, indem Ihre Surfdaten an Dritte weitergegeben werden.

Hier hilft Ihnen die **Cookie-Kontrolle**. Wenn Sie aktiviert ist, wird die **Cookie-Kontrolle** bei jedem Versuch einer Webseite, einen Cookie anzubringen, Ihr diesbezügliches Einverständnis abfragen:



Cookie-Alarm

Der Name des Programms, das versucht einen Cookie zu senden, wird Ihnen angezeigt.

Klicken Sie **Ja** oder **Nein** und eine Regel wird erstellt werden, zugewiesen und gelistet in der Regeltabelle.

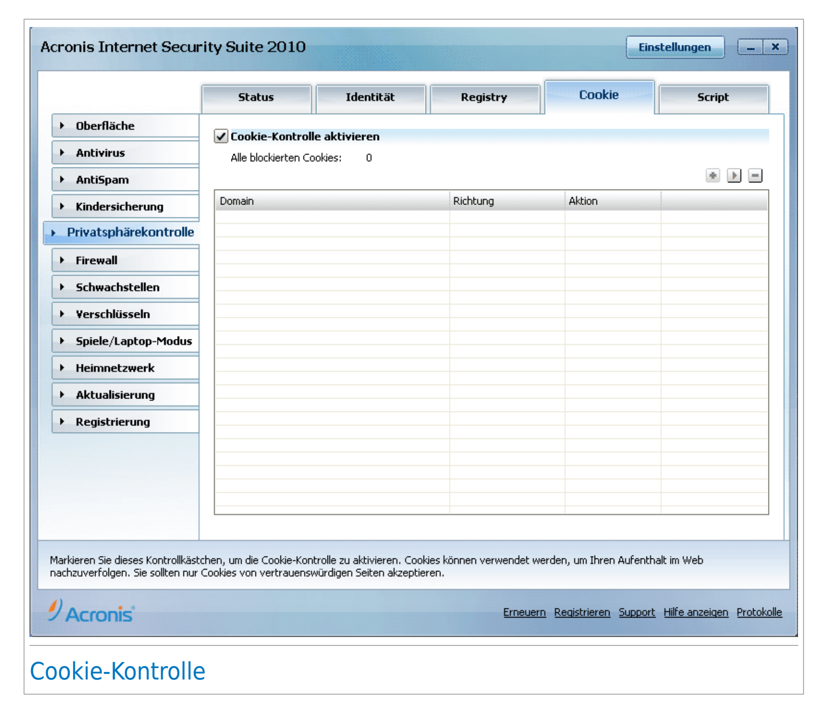
So werden Sie bei der Unterscheidung von zuverlässigen und unzuverlässigen Webseiten unterstützt.



Anmerkung

Aufgrund der großen Anzahl von Cookies, die heute im Internet verwendet werden, kann die **Cookie-Kontrolle** zu Beginn sehr oft nachfragen. Sobald Sie die von Ihnen regelmäßig besuchten Seiten in die Regelliste aufgenommen haben, wird Ihr Surfen im Internet aber wieder wie zuvor sein.

Um die Cookie-Kontrolle zu konfigurieren klicken Sie auf **Privatssphäre>Cookie** in der Profiansicht.



Cookie-Kontrolle

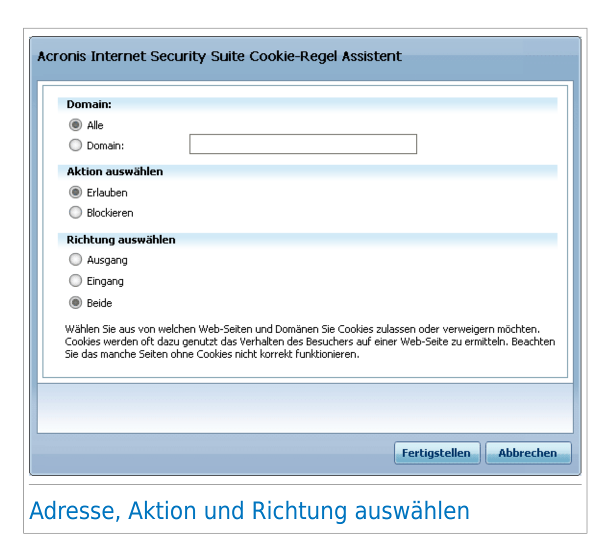
Sie können eine Liste der Regeln in der Aufstellung ansehen.

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche. Zum bearbeiten von Regelparametern, wählen Sie die Regel aus und klicken auf die **Bearbeiten** oder machen Sie einen Doppelklick. Ein neues Fenster erscheint wo Sie die gewünschte konfigurierung durchführen können.

Um eine Regel manuell hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und führen Sie die gewünschten Änderungen in dem Konfigurationsfenster durch.

20.4.1. Konfigurationsfenster

Wenn Sie eine Regel manuell verändern oder hinzufügen, wird ein Konfigurationsfenster erscheinen.



Adresse, Aktion und Richtung auswählen

Hier können Sie die Parameter auswählen:

- **Domäne angeben** - schreiben Sie die Domäne, auf welche die Regel angewendet werden soll, in das darunter stehende Feld.
- **Aktion** - wählen Sie die Aktion der Regel.

Aktion	Beschreibung
Erlauben	Das Cookie dieser Domäne wird ausgeführt.
Verweigern	Das Cookie dieser Domäne wird nicht ausgeführt.

- **Richtung** - Wählen Sie die Richtung des Datenverkehrs aus.

Typ	Beschreibung
Ausgehend	Die Regel bezieht sich nur auf Cookies, welche von der verbundenen Seite versendet werden.
Eingehend	Die Regel bezieht sich nur auf Cookies welche an die verbundene Seite versendet werden.
Beide	Die Regeln finden in beide Richtungen Anwendung.



Anmerkung

Sie können Cookies akzeptieren, diese aber nicht zurücknehmen, indem Sie die Aktion **Verweigern** und die Richtung **Ausgehend** angeben.

Klicken Sie auf **Fertigstellen**.

20.5. Skript-Kontrolle

Skripte und andere Programmierungen, wie z. B. ActiveX und Java applets, die für interaktive Webseiten verwendet werden, können verheerende Schäden verursachen. ActiveX-Elemente können zum Beispiel Zugriff auf Ihre Daten erlangen und sie auslesen, Daten von Ihrem Computer löschen, Passwörter auslesen und Nachrichten versenden, wenn Sie online sind. Sie sollten daher solche aktiven Elemente nur von Ihnen bekannten und zuverlässigen Seiten akzeptieren.

Acronis Internet Security Suite 2010 ermöglicht Ihnen die Auswahl solche Elemente zuzulassen oder deren Ausführung zu blockieren.

Mit der **Skript Kontrolle** entscheiden Sie, welche Webseiten Sie als zuverlässig erachten und welche nicht. Acronis Internet Security Suite 2010 wird immer Ihr Einverständnis abfragen, wenn eine Webseite ein Skript oder einen anderen aktiven Inhalt aktivieren will:

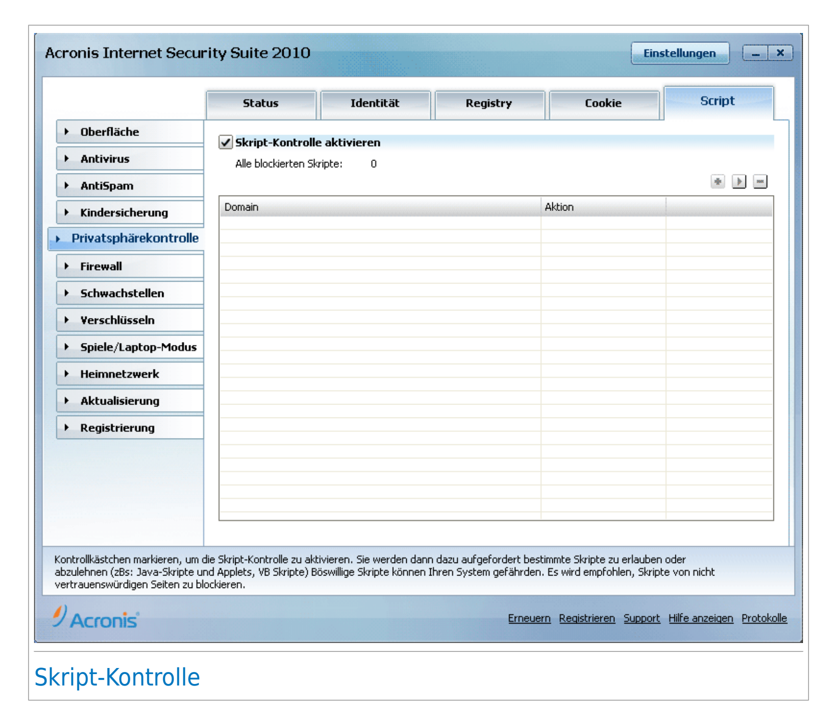


Skript-Alarm

Der Namen der Quelle wird Ihnen angezeigt.

Klicken Sie **Ja** oder **Nein** und eine Regel wird erstellt werden, zugewiesen und gelistet in der Regeltabelle.

Um die Skript-Kontrolle zu konfigurieren klicken Sie auf **Privatssphäre>Skript** in der Profiansicht.



Skript-Kontrolle

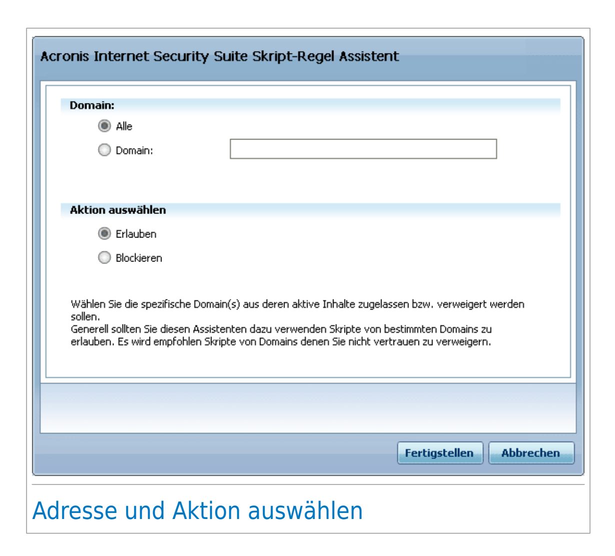
Sie können eine Liste der Regeln in der Aufstellung ansehen.

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche. Zum bearbeiten von Regelparametern, wählen Sie die Regel aus und klicken auf die **Bearbeiten** oder machen Sie einen Doppelklick. Ein neues Fenster erscheint wo Sie die gewünschte konfigurierung durchführen können.

Um eine Regel manuell zu erstellen, klicken Sie auf die Schaltfläche **Hinzufügen** und führen Sie die gewünschten Änderungen im Konfigurationsfenster durch.

20.5.1. Konfigurationsfenster

Wenn Sie eine Regel manuell verändern oder hinzufügen, wird ein Konfigurationsfenster erscheinen.



Adresse und Aktion auswählen

Hier können Sie die Parameter auswählen:

- **Domäne angeben** - schreiben Sie die Domäne, auf welche die Regel angewendet werden soll, in das darunter stehende Feld.
- **Aktion** - wählen Sie die Aktion der Regel.

Aktion	Beschreibung
Erlauben	Die Scripts auf dieser Domäne werden ausgeführt.
Verweigern	Die Scripts auf dieser Domäne werden nicht ausgeführt.

Klicken Sie auf **Fertigstellen**.

21. Firewall

Die Firewall schützt Ihren Computer vor unberechtigten eigehenden und ausgehenden Zugriffen. Sie überwacht Ihre Verbindung und lässt Sie Regeln definieren, welche Verbindung erlaubt ist und welche geblockt werden soll.



Anmerkung

Die Firewall ist ein unersetzliches Instrument bei einer DSL- oder Breitbandverbindung.

Im Stealth-Modus wird ihr Computer im Netzwerk so gut wie unsichtbar vor Angriffen jeglicher Art. Das Firewall-Modul ist in der Lage Portscans zu erkennen und diese gezielt ins Leere laufen zu lassen - so als ob der Computer gar nicht existierte.

21.1. Einstellungen

Um die Firewall zu konfigurieren klicken Sie auf **Firewall>Einstellungen** in der Profiansicht.



Firewall-Einstellungen

Sie können sehen ob ob die Acronis Internet Security Suite 2010 Firewall aktiviert oder deaktiviert ist. Wenn Sie den Status der Firewall ändern möchten, markieren Sie das entsprechende Kontrollkästchen oder lassen Sie es frei.



Wichtig

Um den Schutz vor Angriffen aus dem Internet zu gewährleisten, halten Sie Ihre **Firewall** Funktion jederzeit aktiviert.

Es gibt zwei verschiedene Informationskategorien:

- **Netzwerkkonfiguration.** Sie können den Namen Ihres Computers, seine IP-Adresse und die Standard-Schnittstelle sehen. Wenn Sie mehr als einen Netzwerkadapter haben (dies bedeutet, dass Sie mit mehreren Netzwerken verbunden sind), so sehen Sie die für jeden Adapter konfigurierte IP-Adresse und Schnittstelle.
- **Statistik.** Sie können verschiedene Statistiken zu der Aktivität der Firewall sehen:
  - Anzahl der gesendeten Bytes.
  - Anzahl der empfangenen Bytes.
  - Anzahl der Portscans, die von Acronis Internet Security Suite 2010 entdeckt und blockiert wurden. Portprüfungen werden häufig von Hackern verwendet, um offene Ports auf Ihrem Computer zu finden, um diese dann zu verwenden.
  - Anzahl der abgenommenen Datenpakete.
  - Anzahl der offenen Ports.
  - Anzahl der aktiven Verbindungen mit eingehendem Datenverkehr.
  - Anzahl der aktiven Verbindungen mit ausgehendem Datenverkehr.

Um die aktiven Verbindungen und die offenen Ports zu sehen, klicken Sie auf den Tab Aktivität.

Im unteren Bereich der Maske können Sie eine Statistik bezüglich des eingehenden und ausgehenden Datentransfers beobachten. Diese Grafik zeigt Ihnen das Volumen des Datentransfers über die letzten zwei Minuten an.



Anmerkung

Diese Grafik erscheint auch bei deaktivierter **Firewall**.

21.1.1. Standardaktion einstellen

Standardmäßig erlaubt Acronis Internet Security Suite 2010 automatisch allen Programmen der Whitelist eine Verbindung zum Netzwerk und dem Internet herzustellen. Für alle anderen Programme fordert Sie Acronis Internet Security Suite 2010 über ein Benachrichtigungsfenster dazu auf, die durchzuführende Aktion

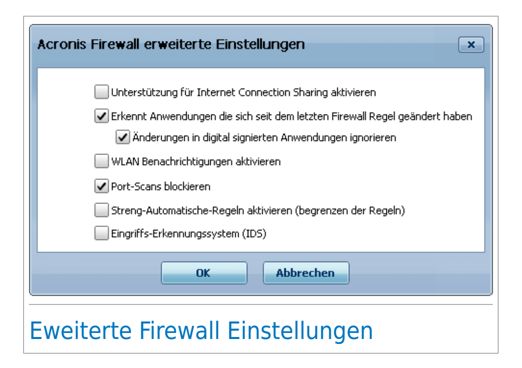
festzulegen. Die von Ihnen festgelgte Aktion wird dann immer durchgeführt, wenn das entsprechende Programm versucht auf das Netzwerk/Internet zuzugreifen.

Ziehen Sie den Zeiger an der Skala entlang um die Standardaktion einzustellen, die durchgeführt werden soll, wenn das Programm versucht auf das Netzwerk/Internet zuzugreifen. Folgende Standardaktionen stehen zur Verfügung:

Standardaktion	Beschreibung
Alle erlauben	Verwendet die momentanen Regeln und erlaubt alle Anfragen welche nicht den Regeln entsprechen ohne Nachfrage. Diese Einstellung kann für Netzwerkadministratoren und Gamer hilfreich sein.
Bekannte Programme erlauben	Wendet die aktuellen Regeln an und erlaubt, ohne vorher zu fragen, alle ausgehenden Verbindungsversuche von Programmen, die in der Whitelist vorhanden sind. Bei anderen Anwendungen werden Sie um Erlaubnis gefragt. Programme mit Freundleslisten sind die am weitesten verbreiteten Programme weltweit. Sie beinhalten die bekanntesten Web Browsers, audio&video Players, Chat und Filesharing Programme, ebenso wie Server Clients und Betriebssystem Anwendungen. Um die Freundesliste sehen zu können, klicken Sie auf **Freundesliste anzeigen**.
Berichte	Verwendet die momentanen Regeln und frägt Sie bei alle Anfragen welche nicht den Regeln entsprechen.
Alle verweigern	Wendet die aktuellen Regeln an und verweigert alle Verbindungsversuche, wenn diese nicht mit den aktuellen Regeln übereinstimmen.

21.1.2. Weitere Einstellungen der Firewall konfigurieren

Sie können auf **Erweitert** klicken, um die erweiterten Firewall-Einstellungen zu konfigurieren.



Eweiterte Firewall Einstellungen

Die folgenden Optionen sind verfügbar:

- **Unterstützung für Internet Connection Sharing aktivieren** - Erlaubt die Unterstützung von Internet Connection Sharing (ICS).



Anmerkung

Diese Option erlaubt nicht automatisch ICS auf Ihrem System sondern erlaubt diese Art von Verbindung nur, wenn Sie es von Ihrem Betriebssystem aus freigeben.

Internet Connection Sharing (ICS) erlaubt es Anwendern in lokalen Netzwerken von ihrem Computer aus auf das Internet zuzugreifen. Dies ist sinnvoll wenn Sie eine spezielle/bestimmte Internet Verbindung(z.B. Drahtlose Anbindung) nutzen und diese mit anderen Mitgliedern im Netzwerk teilen wollen.

Das Teilen von Internet Verbindungen mit anderen Mitgliedern im lokalen Netzwerk für zu einem höheren Ressourcen Verbrauch und birgt gewisse Risiken. Es belegt zudem einige Ihrer Ports (solche die von den Mitgliedern geöffnet werden, die die Internet Verbindung nutzen).

- **Finde Anwendungen die sich seit dem Erstellen der Firewall-Regel verändert haben** - prüft jede Anwendung die versucht eine Verbindung zum Internet herzustellen, um zu erkennen ob sich bei dieser seit dem Hinzufügen der Regel, die den Zugriff überwacht, etwas verändert hat. Falls sich etwas verändert hat, wird eine Warnung Sie auffordern den Zugriff zu erlauben oder zu blockieren.

Normalerweise werden Anwendungen durch Updates verändert, es kann aber auch sein das eine Anwendung durch einen Schädling verändert wird um Ihren Computer zu infizieren.



Anmerkung

Wir empfehlen Ihnen die Option aktiviert zu lassen und nur Anwendungen Zugriff zu gewähren bei welchen Sie erwarten das diese Zugriff zum Internet benötigen.

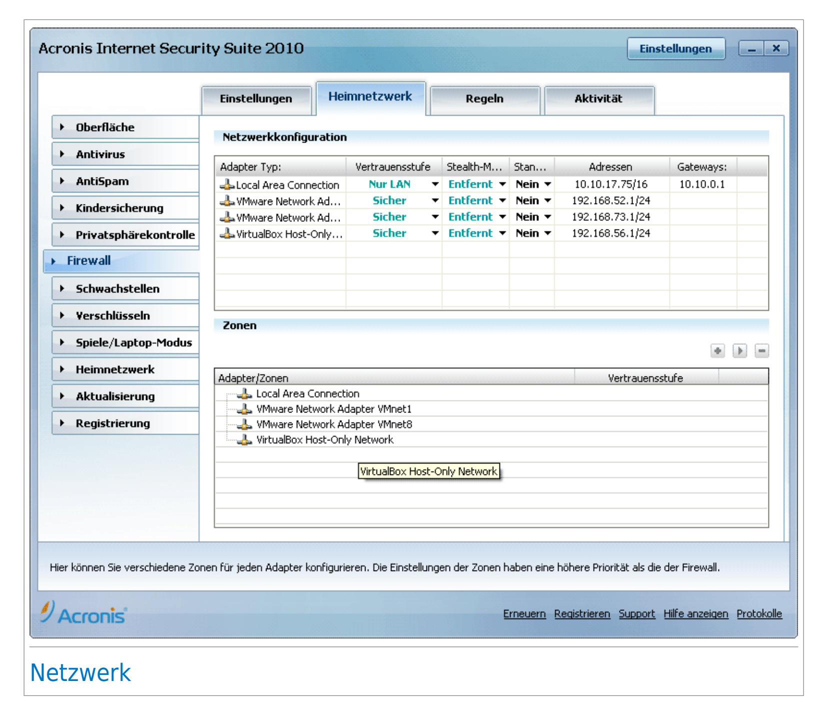
Signierte Anwendungen sind in normalerweise vertrauenswürdig und haben einen höheren Sicherheitsgrad. Signierte Anwendungen haben einen höheren Sicherheitsfaktor. Sie können diesen Anwendungen den Zugriff erlauben auch wenn diese verändert wurden. Aktivieren Sie hierzu die Option **Änderungen bei signierten Prozessen ignorieren**.

- **WLAN Benachrichtigungen aktivieren** - wenn Sie mit einem drahtlosen Netzwerk verbunden sind, werden Informationsfenster bezüglich bestimmter Netzwerkereignisse angezeigt (z.B. wenn ein neuer Computer dem Netzwerk beitritt).
- **Portscans blockieren** - entdeckt und blockiert Versuche offene Ports zu finden.

  Portscans werden von Hackern verwendet, um herauszufinden, welche Ports auf Ihrem Computer geöffnet sind. Wenn Sie dann einen unsicheren Port finden, können Sie in Ihren Computer eindringen.
- **Genaue automatische Regeln** -erstellt genaue Regeln bezüglich der Verwendung des Benachrichtigungsfensters der Firewall. Wenn diese Option ausgewählt ist, wird Acronis Internet Security Suite 2010 Sie dazu auffordern für jede Anwendung, die versucht auf das Netzwerk oder das Internet zuzugreifen, eine Aktion durchzuführen und Regeln zu erstellen.
- **Intrusion detection system (IDS)** - aktiviert die heuristische Überwachung von Anwendungen, die versuchen auf das Netzwerk oder das Internet zuzugreifen.

21.2. Netzwerk

Um die Firewall-Einstellungen zu konfigurieren klicken Sie auf **Firewall>Netzwerk** in der Profiansicht.



Netzwerk

Die Spalten in der Tabelle **Netzwerkkonfiguration** bieten Ihnen detaillierte Informationen über das Netzwerk mit dem Sie verbunden sind:

- **Adapter** - Der Netzwerkadapter, den Ihr Computer verwendet, um eine Verbindung mit dem Netzwerk oder dem Internet herzustellen.
- **Vertrauensstufe** - Die Vertrauensstufe, die dem Netzwerkadapter zugewiesen ist. Entsprechend der Netzwerkadapterkonfiguration wird Acronis Internet Security Suite 2010 dem Adapter automatisch eine Vertauensstufe zuweisen oder Sie nach weiteren Angaben fragen.
- **Stealth Modus** - Ob Sie von anderen Computern entdeckt werden können.
- **Generisch** - Ob für diese Verbindung generische Regeln angewendet werden.
- **Adressen** - die für den Adapter konfigurierte IP-Adresse.
- **Schnittstellen** - Die IP-Adresse die Ihr Computer verwendet um eine Verbindung mit dem Internet herzustellen.

21.2.1. Vertrauensstufe ändern

Acronis Internet Security Suite 2010 weist jedem Netzwerkadapter eine Vertrauensstufe zu. Die Vertrauensstufe, die einem Adapter zugewiesen ist zeigt an, wie vertrauenswürdig das entsprechende Netzwerk ist.

Basierend auf der Vertrauensstufe werden verschiedene Reglen für den Adapter erstellt, bezüglich des Umgangs von Acronis Internet Security Suite 2010 und des Systems mit dem Zugang zum Netzwerk oder Internet.

Sie können die für jeden Adapter konfigurierte Vertrauensstufe in der Tabelle **Netzwerkkonfiguration** in der Spalte **Vertrauensstufe** sehen. Um die Vertrauensstufe zu ändern, klicken Sie auf den Pfeil der Spalte **Vertrauensstufe** und wählen Sie die gewünschte Stufe.

Vertrauensstufe	Beschreibung
Vollkommen vertrauenswürdig	Deaktiviert die Firewall für den entsprechenden Adapter.
Lokal vertrauenswürdig	Erlaubt den Datenverkehr zwischen Ihrem Computer und den Computern im lokalen Netzwerk.
Sicher	Erlaubt das gemeinsame Verwenden von Ressourcen mit Computern im lokalen Netzwerk. Diese Stufe ist für lokale Netzwerke (im Haushalt oder Büro) automatisch eingestellt.
Unsicher	Netzwerk- oder Internet-Computer können keine Verbindung mit Ihrem Computer herstellen. Diese Stufe ist für öffentliche Netzwerke (wenn Sie eine IP-Adresse von einem Internet Service Provider erhalten haben) automatisch eingestellt.
Lokal blockieren	Blockiert jeglichen Datenverkehr zwischen Ihrem Computer und Computern im lokalen Netzwerk, während der Internetzugang bestehen bleibt. Diese Vertrauensstufe ist automatisch für unsichere (offene) WLAN-Netzwerke eingestellt.
Blockiert	Der Netzwerk- und Internet-Datenverkehr über den entsprechenden Adapter wird vollständig blockiert.

21.2.2. Den Stealth-Modus konfigurieren

Der Stealth-Modus macht Ihren Computer unsichtbar für schädliche Software und Hacker im Netzwerk oder Internet. Um den Stealth-Modus zu konfigurieren, klicken Sie auf den Pfeil ▾ in der Spalte **Verdeckt** und wählen Sie die gewünschte Option.

Stealth-Option	Beschreibung
Einschalten	Stealth-Modus ist aktiviert. Ihr Computer ist weder im lokalen Netzwerk noch im Internet sichtbar.
Ausschalten	Stealth-Modus ist deaktiviert. Jeder Benutzer im lokalen Netzwerk oder im Internet kann Ihren Computer entdecken.
Remote	Ihr Computer kann nicht im Internet entdeckt werden. Benutzer im lokalen Netzwerk können Ihren Computer entdecken

21.2.3. Generische Einstellungen vornehmen

Wenn sich die IP-Adresse eines Netzwerkadapters geändert hat, verändert Acronis Internet Security Suite 2010 die Vertrauensstufe entsprechend. Wenn Sie die selbe Vertrauensstufe beibehalten möchten, klicken Sie auf den Pfeil in der Spalte **Generisch** und wählen Sie **Ja**.

21.2.4. Netzwerk-Zonen

Sie können erlaubte oder blockierte Computer für einen bestimmten Adpater hinzufügen.

Ein vertrauenswürdiger Bereich ist ein Computer, dem Sie vollständig vertrauen. Zwischen Ihrem Computer und den Computern, denen Sie vertrauen, ist jeglicher Datenaustausch erlaubt. Um Ressourcen mit speziellen Computern in ungesicherten WLAN-Netzwerken zu teilen, fügen Sie sie als erlaubte Computer hinzu.

Ein blockierter Bereich ist ein Computer, mit dem Ihr Computer in keiner Weise kommunizieren soll.

Die Tabelle **Bereiche** zeigt die aktuellen Netzwerkbereiche für jeden Adampter an.

Um einen Bereich hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen**.



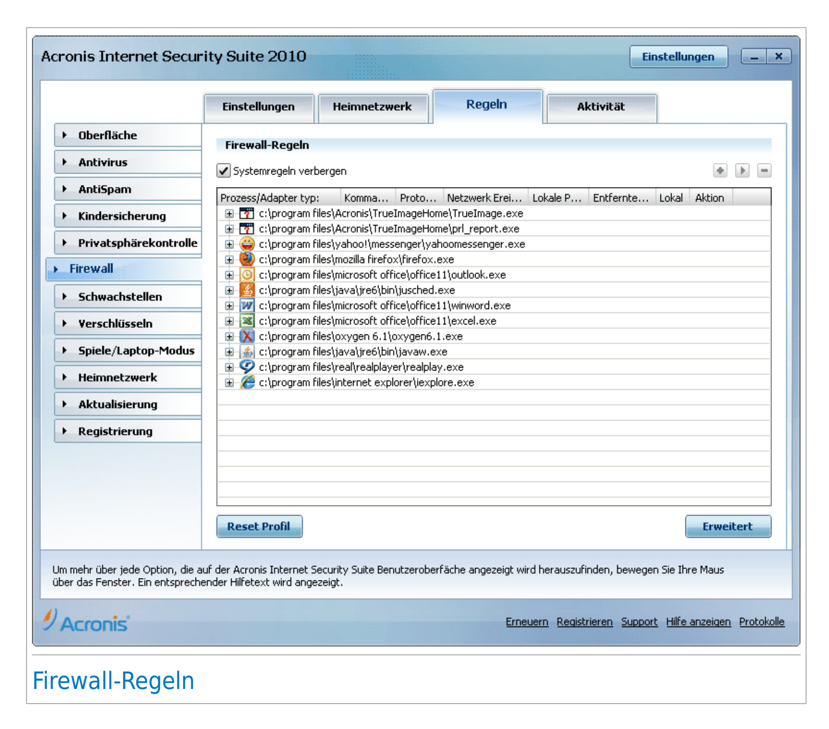
Bereich hinzufügen

Gehen Sie wie folgt vor:

1. Wählen Sie die IP-Adresse des Computers der hinzugefügt werden soll.
2. Wählen Sie eine Aktion:
   - **Erlauben** - jeglicher Datenverkehr zwischen Ihrem Computer und dem ausgewählten Computer wird erlaubt.
   - **Verweigern** - jeglicher Datenverkehr zwischen Ihrem Computer und dem ausgewählten Computer wird blockiert.
3. Klicken Sie auf **OK**.

21.3. Regeln

Um die Firewall Regeln, die den Netzwerk- und Internetzugriff von Programmen kontrollieren, zu konfigurieren, klicken Sie auf **Firewall>Regeln** in der Profiansicht.



Firewall-Regeln

Sie können die Programme (Prozesse) sehen, für die die Firewall-Regel erstellt wurde. Lassen Sie das Kontrollkästchen **Systemregeln verbergen** frei, wenn Sie ebenfalls die Regeln bezüglich des Systems oder von Acronis Internet Security Suite 2010 Prozessen zu sehen.

Um die Regeln zu sehen, die für eine bestimmte Anwendung erstellt wurden, klicken Sie auf das + Kästchen neben der entsprechenden Anwendung. Sie können detaillierte Informationen für jede Regel sehen, so wie sie in den Spalten der Tabelle dargestellt sind:

- **Prozess/Adapter-Typen** - der Prozess und die Netzwerkadaptertypen für die die Regel angewendet wird. Regeln werden automatisch erstellt um den Netzwerk- oder Internetzugriff jedes Adapters zu filtern. Sie können manuell Regeln erstellen oder bestehende Regeln bearbeiten um den Zugriff einer Anwendung auf das Netzwerk/Internet über einen speziellen Adapter zu filtern (zum Beispiel ein drahtloser Netzwerkadapter).
- **Befehlszeile** - der Befehl in der Windows Befehlszeile der verwendet wird um den Prozess zu starten (**cmd**).
- **Protokoll** - das IP-Protokoll für das die Regel angewendet wird. Sie werden eines der Folgenden sehen:

Protokoll	Beschreibung
Alle	Beinhaltet alle IP-Protokolle.
TCP	Transmission Control Protocol (TCP) ist eine Vereinbarung (Protokoll) darüber, auf welche Art und Weise Daten zwischen Computern ausgetauscht werden sollen. Alle am Datenaustausch beteiligten Computer kennen diese Vereinbarungen und befolgen sie. Es ist damit ein zuverlässiges, verbindungsorientiertes Transportprotokoll in Computernetzwerken. Es ist Teil der TCP/IP-Protokollfamilie. Entwickelt wurde TCP von Robert E. Kahn und Vinton G. Cerf. Ihre Forschungsarbeit, die sie im Jahre 1973 begannen, dauerte mehrere Jahre. Die erste Standardisierung von TCP erfolgte deshalb erst im Jahre 1981 als RFC 793. TCP stellt einen virtuellen Kanal zwischen zwei Endpunkten einer Netzwerkverbindung (Sockets) her. Auf diesem Kanal können in beide Richtungen Daten übertragen werden. TCP setzt in den meisten Fällen auf das IP-Protokoll auf. Es ist in Schicht 4 des OSI-Referenzmodells angesiedelt.
UDP	User Datagram Protocol (UDP) ist ein minimales, verbindungsloses Netzprotokoll. Es gehört zur Transportschicht der TCP/IP-Protokollfamilie und ist im Gegensatz zu TCP nicht auf Zuverlässigkeit ausgelegt. UDP erfüllt im Wesentlichen den Zweck, die durch die IP-Schicht hergestellte Endsystemverbindung um eine Anwendungsschnittstelle (Ports) zu erweitern. Die Qualität der darunter liegenden Dienste, insbesondere die Zuverlässigkeit der Übertragung, erhöht UDP hingegen nicht.
Eine Nummer	Stellt ein besonderes IP-Protokoll dar (anders als TCP und UDP). Die komplette Liste zugewiesener Nummern von IP-Protokollen finden Sie unter www.iana.org/assignments/protocol-numbers.

- **Netzwerkereignisse** - die Netzwerkereignisse für die die Regel angewendet wird. Folgende Ereignisse können auftreten:

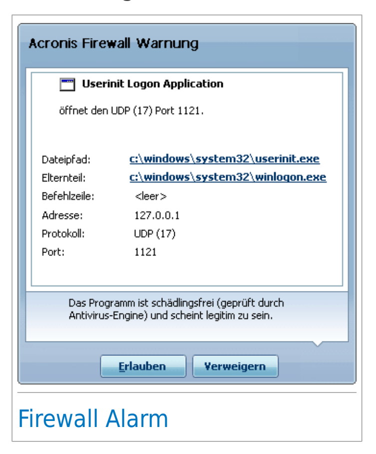
Ereignis	Beschreibung
Verbinden	Vorausgehender Austausch von Standardnachrichten, die von Verbindungsprotokollen (wie TCP) verwendet werden, um eine Verbindung herzustellen. Mit Verbindungsprotokollen entsteht ein Datenverkehr zwischen zwei Computern nur nachdem eine Verbindung hergestellt wurde.

Ereignis	Beschreibung
Datenverkehr	Datenfluss zwischen zwei Computern.
Überwachen	Status in dem eine Anwendung das Netzwerk überwacht, das eine Verbindung herstellen oder Informationen über eine Peer-Anwendung erhalten möchte.

- **Lokale Ports** - die Ports auf Ihrem Computer, für die die Regel angewendet wird.
- **Remote-Ports** - die Ports auf den Remote-Computern, für die die Regel angewendet wird.
- **Lokal** - ob die Regel nur für Computer im lokalen Netzwerk angewendet wird.
- **Aktion** - ob der Anwendung unter den festgelegten Umständen der Zugriff auf das Netzwerk/Internet erlaubt oder verweigert wird.

21.3.1. Regeln automatisch hinzufügen

Bei aktivierter **Firewall** fragt Acronis Internet Security Suite 2010 bei jedem Verbindungsaufbau zum Internet ab, ob diese zugelassen werden soll:



Firewall Alarm

Sie können folgendes sehen: Die Anwendung, die versucht, auf das Internet, den Pfad zur Anwendungsdatei, dem Bestimmungsort, das Protokoll verwendet und Port , auf dem die Anwendung versucht in Verbindung zu stehen.

Wählen Sie **Erlauben** um allen Datenverkehr für diese Anwendung über das eingestellt Protokol zu erlauben (eingehend und ausgehend). Wenn Sie **Verweigern**wählen, wird der Zugriff entsprechend blockiert.

Bassierend auf Ihrer Wahl wird eine Regel erstellt. Das nächste Mal wenn die Anwendung versucht eine Verbindung herzustellen wird die Regeln direkt angewand.



Wichtig

Erlauben Sie nur eingehende Verbindungen von IP-Adressen oder Internet-Domänen, denen Sie wirklich vertrauen.

21.3.2. Löschen und Zurücksetzen von Regeln

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche. Sie können eine oder auch mehrere Regeln auswählen und löschen.

Wenn Sie alle Regeln die für eine bestimmte Anwendung erstellt wurden löschen möchten, wählen Sie die Anwendung aus der Liste und klicken Sie auf die **Regel löschen**-Schaltfläche.

Falls Sie für die gewählte Vertrauensstufe den Standardregelsatz laden wollen, klicken Sie **Regeln Zurücksetzen**.

21.3.3. Regeln erstellen und bearbeiten

Durch das Konfigurieren der Regelparameter im Konfigurationsfenster können neue Regeln erstellt und bestehende Regeln bearbeitet werden.

Regeln erstellen. Um eine Regel manuell zu erstellen, befolgen Sie folgende Schritte:

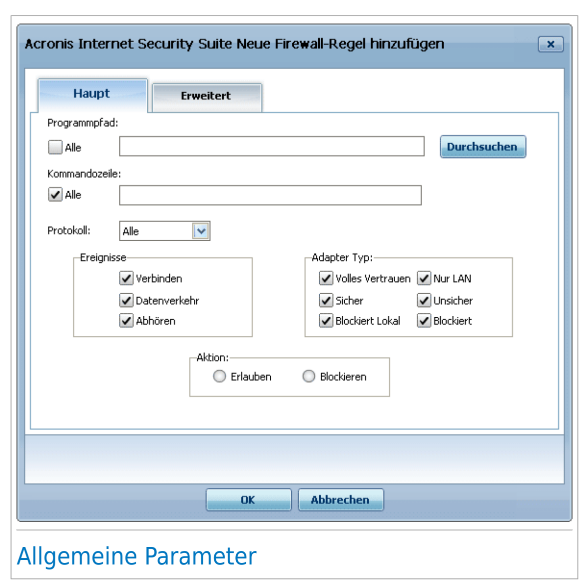
1. Klicken Sie auf die **Regel hinzufügen** -Schaltfläche. Das Konfigurationsfenster wird erscheinen.
2. Knofigurieren Sie die wichtigsten und erweiterten Parameter wie benötigt.
3. Klicken Sie auf **OK** um die neue Regel hinzuzufügen.

Regeln bearbeiten. Um eine bestehende Regel zu bearbeiten, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **Regel bearbeiten** oder doppelklicken Sie auf die Regel. Das Konfigurationsfenster wird erscheinen.
2. Knofigurieren Sie die wichtigsten und erweiterten Parameter wie benötigt.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Allgemeine Parameter konfigurieren

Der Tab **Allgemein** des Konfigurationsfensters bietet Ihnen die Möglichkeit die allgemeinen Regelparameter zu verwalten.



Allgemeine Parameter

Folgende Parameter können konfiguriert werden:

- **Programmpfad.** Klicken Sie auf **Durchsuchen** und wählen Sie das Programm für das die Regel angewendet wird. Wenn Sie möchten, dass die Regel für alle Programme angewendet wird, wählen Sie **Alle**.
- **Befehlszeile.** Wenn Sie möchten, dass die Regel nur angewendet wird, wenn die ausgewählte Anwendung mit einem bestimmten Befehl in der Befehlszeile von Windows geöffnet wird, lassen Sie das Kontrollkästchen **Alle** frei und geben Sie den entsprechenden Befehl in das Editierfeld ein.
- **Protokoll.** Wählen Sie aus dem Menu das IP-Protokoll für das die Regel angewendet wird.
  - ▶ Wenn Sie möchten, dass die Regel für alle Protokolle angewendet wird, wählen Sie **Alle**.
  - ▶ Wenn Sie möchten, dass die Regel für TCP-Protokolle angewendet wird, wählen Sie **TCP**.
  - ▶ Wenn Sie möchten, dass die Regel für UDP-Protokolle angewendet wird, wählen Sie **UDP**.
  - ▶ Wenn Sie möchten, dass die Regel für ein bestimmtes Protokoll angewendet wird, wählen Sie **Andere**. Ein Editierfeld wird erscheinen. Geben Sie die dem Protokoll, das gefiltert werden soll, zugewiesene Nummer in das Editierfeld ein.



Anmerkung

Die Nummern von IP-Protokollen werden von der Internet Assigned Numbers Authority (IANA) zugewiesen. Die komplette Liste zugewiesener Nummern von IP-Protokollen finden Sie unter www.iana.org/assignments/protocol-numbers.

- **Ereignisanzeige.** Wählen Sie je nach ausgewähltem Protokoll die Netzwerkereignisse, für die die Regel angewendet werden soll. Folgende Ereignisse können auftreten:

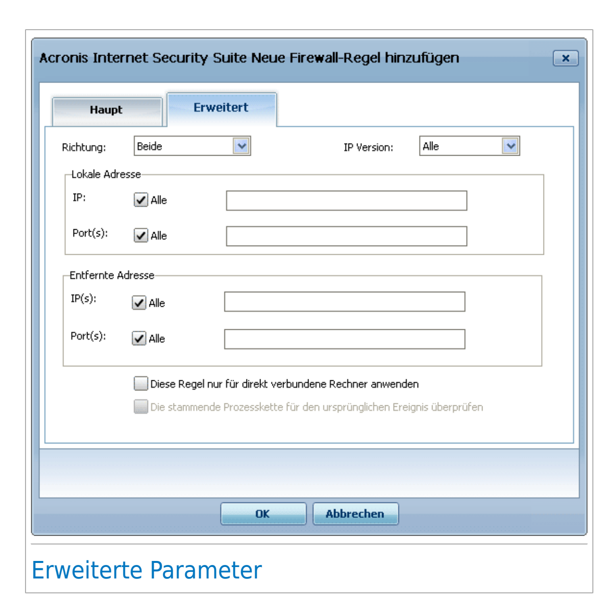
Ereignis	Beschreibung
Verbinden	Vorausgehender Austausch von Standardnachrichten, die von Verbindungsprotokollen (wie TCP) verwendet werden, um eine Verbindung herzustellen. Mit Verbindungsprotokollen entsteht ein Datenverkehr zwischen zwei Computern nur nachdem eine Verbindung hergestellt wurde.
Datenverkehr	Datenfluss zwischen zwei Computern.
Überwachen	Status in dem eine Anwendung das Netzwerk überwacht, das eine Verbindung herstellen oder Informationen über eine Peer-Anwendung erhalten möchte.

- **Adapter Typ.** Wählen Sie den Adaptertyp aus, für die diese Regel angewendet werden soll:
- **Aktion.** Folgende Aktionen sind wählbar:

Aktion	Beschreibung
Erlauben	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen erlaubt.
Verweigern	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen verweigert.

Erweiterte Parameter konfigurieren

Der Tab **Erweitert** des Konfigurationsfensters gibt Ihnen die Möglichkeit erweiterte Regelparameter zu konfigurieren.



Erweiterte Parameter

Folgende erweiterte Parameter können konfiguriert werden:

- **Richtung.** Wählen Sie aus dem Menu die Richtung des Datenverkehrs, für den die Regel angewendet wird.

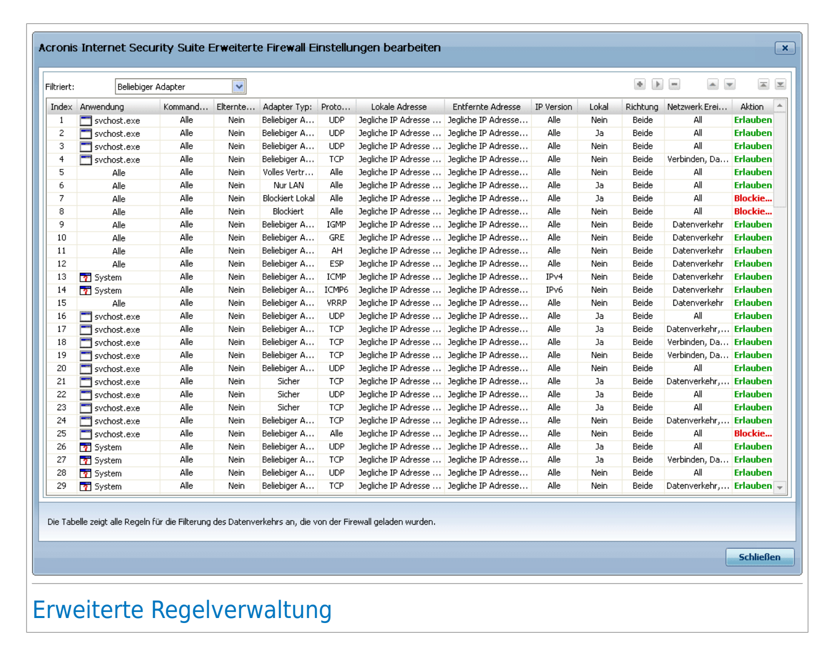
Richtung	Beschreibung
Ausgehend	Die Regeln beziehen sich nur auf ausgehenden Datenverkehr.
Eingehend	Die Regeln beziehen sich nur auch eingehenden Datenverkehr.
Beide	Die Regeln finden in beide Richtungen Anwendung.

- **IP-Version.** Wählen Sie aus dem Menu die IP-Version (IPv4, IPv6 oder andere), für die die Regel angewendet werden soll.
- **Lokale Adresse.** Bestimmen Sie die lokale IP-Adresse und den Port, für die die Regel angewendet werden soll, wie folgt:
  - ▶ Wenn Sie mehr als einen Netzwerkadapter haben, können Sie das Kontrollkästchen **Alle** freilassen und eine bestimmte IP-Addresse eingeben.
  - ▶ Falls Sie TCP oder UDP als Protokoll ausgewählt haben, können Sie spezielle Ports in der Bandbreite von 0 und 65535 auswählen. Wenn Sie die definierten Regeln für alle Ports auswählen möchten, wählen Sie bitte **Alle**.

- **Entfernte Adresse.** Bestimmen Sie die Remote-IP-Adresse und den Port, für die die Regel angewendet werden soll, wie folgt:
  - ▶ Um den Datenverkehr zwischen Ihrem Computer und einem bestimmten Computer zu filtern, lassen Sie das Kontrollkästchen **Alle** frei und geben Sie dessen IP-Adresse an.
  - ▶ Falls Sie TCP oder UDP als Protokoll ausgewählt haben, können Sie spezielle Ports in der Bandbreite von 0 und 65535 auswählen. Wenn Sie die definierten Regeln für alle Ports auswählen möchten, wählen Sie bitte **Alle**.
- **Diese Regel nur für direkt verbundene Computer anwenden.** Wählen Sie diese Option, wenn Sie möchten dass diese Regel nur für den lokalen Datenverkehr angewendet werden soll.
- **Den Ablauf überprüfen um das ursprüngliche Ereignis festzustellen.** Sie können diesen Parameter nur verändern, wenn Sie **Genaue automatische Regeln** ausgewählt haben (öffnen Sie den Tab Einstellungen und klicken Sie auf **Erweiterte Einstellungen**). Genaue Regeln bedeuten, dass Acronis Internet Security Suite 2010 Sie auffordert eine Aktion durchzuführen, wenn eine Anwendung versucht eine Verbindung mit dem Netzwerk/Internet herzustellen, wenn der vorangegangene Prozess ein anderer war.

21.3.4. Erweiterte Regelverwaltung

Wenn Sie eine erweiterte Kontrolle über die Firewall-Regeln benötigen, klicken Sie auf **Erweitert**. Ein neues Fenster wird sich öffnen.



Acronis Internet Security Suite Erweiterte Firewall Einstellungen bearbeiten

Filtriert: Beliebiger Adapter

Index	Anwendung	Kommand...	Elternte...	Adapter Typ:	Proto...	Lokale Adresse	Entfernte Adresse	IP Version	Lokal	Richtung	Netzwerk Erei...	Aktion
1	svchost.exe	Alle	Nein	Beliebiger A...	UDP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	All	Erlauben
2	svchost.exe	Alle	Nein	Beliebiger A...	UDP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Ja	Beide	All	Erlauben
3	svchost.exe	Alle	Nein	Beliebiger A...	UDP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	All	Erlauben
4	svchost.exe	Alle	Nein	Beliebiger A...	TCP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	Verbinden, Da...	Erlauben
5	Alle	Alle	Nein	Volles Vertr...	Alle	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	All	Erlauben
6	Alle	Alle	Nein	Nur LAN	Alle	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Ja	Beide	All	Erlauben
7	Alle	Alle	Nein	Blockiert Lokal	Alle	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Ja	Beide	All	Blockie...
8	Alle	Alle	Nein	Blockiert	Alle	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	All	Blockie...
9	Alle	Alle	Nein	Beliebiger A...	IGMP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	Datenverkehr	Erlauben
10	Alle	Alle	Nein	Beliebiger A...	GRE	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	Datenverkehr	Erlauben
11	Alle	Alle	Nein	Beliebiger A...	AH	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	Datenverkehr	Erlauben
12	Alle	Alle	Nein	Beliebiger A...	ESP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	Datenverkehr	Erlauben
13	System	Alle	Nein	Beliebiger A...	ICMP	Jegliche IP Adresse ...	Jegliche IP Adresse...	IPv4	Nein	Beide	Datenverkehr	Erlauben
14	System	Alle	Nein	Beliebiger A...	ICMP6	Jegliche IP Adresse ...	Jegliche IP Adresse...	IPv6	Nein	Beide	Datenverkehr	Erlauben
15	Alle	Alle	Nein	Beliebiger A...	VRRP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	Datenverkehr	Erlauben
16	svchost.exe	Alle	Nein	Beliebiger A...	UDP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Ja	Beide	All	Erlauben
17	svchost.exe	Alle	Nein	Beliebiger A...	TCP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Ja	Beide	Datenverkehr,...	Erlauben
18	svchost.exe	Alle	Nein	Beliebiger A...	TCP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Ja	Beide	Verbinden, Da...	Erlauben
19	svchost.exe	Alle	Nein	Beliebiger A...	TCP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	Verbinden, Da...	Erlauben
20	svchost.exe	Alle	Nein	Beliebiger A...	UDP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	All	Erlauben
21	svchost.exe	Alle	Nein	Sicher	TCP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Ja	Beide	Datenverkehr,...	Erlauben
22	svchost.exe	Alle	Nein	Sicher	UDP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Ja	Beide	All	Erlauben
23	svchost.exe	Alle	Nein	Sicher	TCP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Ja	Beide	All	Erlauben
24	svchost.exe	Alle	Nein	Beliebiger A...	TCP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	Datenverkehr,...	Erlauben
25	svchost.exe	Alle	Nein	Beliebiger A...	Alle	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	All	Blockie...
26	System	Alle	Nein	Beliebiger A...	UDP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Ja	Beide	All	Erlauben
27	System	Alle	Nein	Beliebiger A...	TCP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Ja	Beide	Verbinden, Da...	Erlauben
28	System	Alle	Nein	Beliebiger A...	UDP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	All	Erlauben
29	System	Alle	Nein	Beliebiger A...	TCP	Jegliche IP Adresse ...	Jegliche IP Adresse...	Alle	Nein	Beide	Datenverkehr,...	Erlauben

Die Tabelle zeigt alle Regeln für die Filterung des Datenverkehrs an, die von der Firewall geladen wurden.

Schließen

Erweiterte Regelverwaltung

Sie können eine Liste der Firewall-Regeln, nach dem Datum der Erstellung geordnet, sehen. Die Spalten der Tabelle geben nützliche Informationenzu jeder Regel.



Anmerkung

Wenn ein Verbindungsversuch ausgeführt wurde (sowohl eingehend als auch ausgehend), wendet Acronis Internet Security Suite 2010 die Aktion der ersten Regel an, die auf die entsprechende Verbindung zutrifft. Deshalb ist die Reihenfolge der Regeln sehr wichtig.

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche.

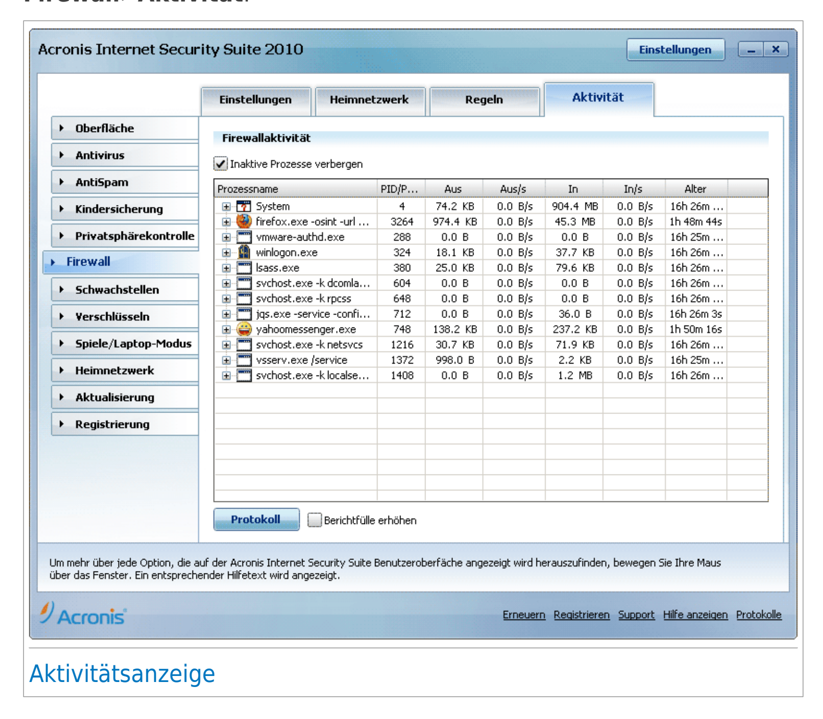
Um eine Regel zu bearbeiten wählen Sie die Regel aus und klicken Sie auf **Bearbeiten**.

Sie können die Priorität einer Regel erhöhen oder heruntersetzen. Klicken Sie **In der Liste hochsetzen** um die ausgewählte Regel um ein Level nach oben zu setzen. Oder klicken Sie **In Liste heruntersetzen** um die Priorität der ausgewählten Regel herunterzusetzen. Um einer Regel die höchste Priorität zu geben klicken Sie auf die **Als erste**-Schaltfläche. Um einer Regel die niedrigste Priotität zu zuweisen klicken Sie auf die **Als letzte**-Schaltfläche.

Klicken Sie auf **Schließen** um dieses Fenster zu schließen.

21.4. Aktivitätsanzeige

Um die aktuellen Netzwerk-/Internetaktivitäten zu verfolgen (TCP und UDP) und um den Firewall-Bericht einzusehen klicken Sie in der Profi-Ansicht auf **Firewall>Aktivität**.



Aktivitätsanzeige

Hier können Sie den Datenvekehr sortiert nach Anwendung einsehen. Für jede Anwendung können Sie die Verbindungen und offenen Ports sehen. Ausserdem Statistiken zum ausgehenden &eingehenden Datenverkehr.

Wenn Sie ebenfalls inaktive Prozesse sehen wollen, lassen Sie das Kontrollkästchen **Inaktive Prozesse verbergen** frei.

Die Bedeutung der Symbole ist wie folgt:

- Zeigt eine ausgehende Verbindung an.
- Zeigt eine eingehende Verbindung an.
- Zeigt einen offenen Port auf Ihrem Computer an.

Das Fenster zeigt die aktuellen Netzwerk/Internetaktivitäten in Echtzeit. Wenn einzelne Verbindungen oder Ports geschlossen werden können Sie sehen wie diese

ausgrauen, und evtl. verschwinden. Das selbe kann auch mit Anwendungen im Fenster geschehen welche geschlossen werden.

Für eine umfangreiche Ereignisliste bezüglich der Verwendung des Firewall-Moduls (Firewall aktivieren/deaktivieren, Datenverkehr blockieren, Einstellungen verändern) oder die durch die von diesem Modul entdeckten Aktivitäten erstellt wurden (Portprüfung, Verbindungsversuche oder Datenverkehr entsprechend den Regeln blockieren), betrachten Sie das Acronis Internet Security Suite 2010 Firewall-Protokoll indem Sie auf **Protokoll anzeigen** klicken.

Wenn Sie möchten, dass das Protokoll noch mehr Informationen enthält, wählen Sie **Protokollumfang erweitern**.

22. Schwachstellen

Ein wichtiger Schritt für den Schutz Ihres Computers gegen Hacker und schädliche Anwendungen besteht darin, das Betriebssystem und die Programme, die Sie oft verwenden, stets auf dem neusten Stand eu halten. Und um einen ungewünschten Zugriff auf Ihren Computer zu vermeiden sind sichere Passwörter (Passwörter die nicht einfach umgangen werden können) für jedes Windows-Benutzerkonto notwendig.

Acronis Internet Security Suite 2010 überprüft Ihr System regelmäßig auf Schwachstellen und benachrichtigt Sie über bestehende Probleme oder Risiken.

22.1. Status

Um die automatische Prüfung auf Schwachstellen zu konfigurieren oder eine Prüfung auf Schwachstellen auszuführen, klicken Sie auf **Schwachstellen>Status** in der Profiansicht.



Status der Schwachstellen Prüfung

Jede Tabelle zeigt die gelöste Objekte aus der letzten Schwachstellen Prüfung und deren aktuellen Status an. Hier können Sie sehen, welche Aktion Sie durchführen

sollen, um jede Schwachstelle zu beheben, falls welche vorhanden. Wenn die Aktion**Keine** ist, dann wird diese Angelegenheit keine Schwachstelle darstellen.



Wichtig

Um automatisch über System- oder Anwendungsschwachstellen benachrichtigt zu werden, lassen Sie die **Automatische Prüfung auf Schwachstellen** aktiviert.

22.1.1. Schwachstellen beheben

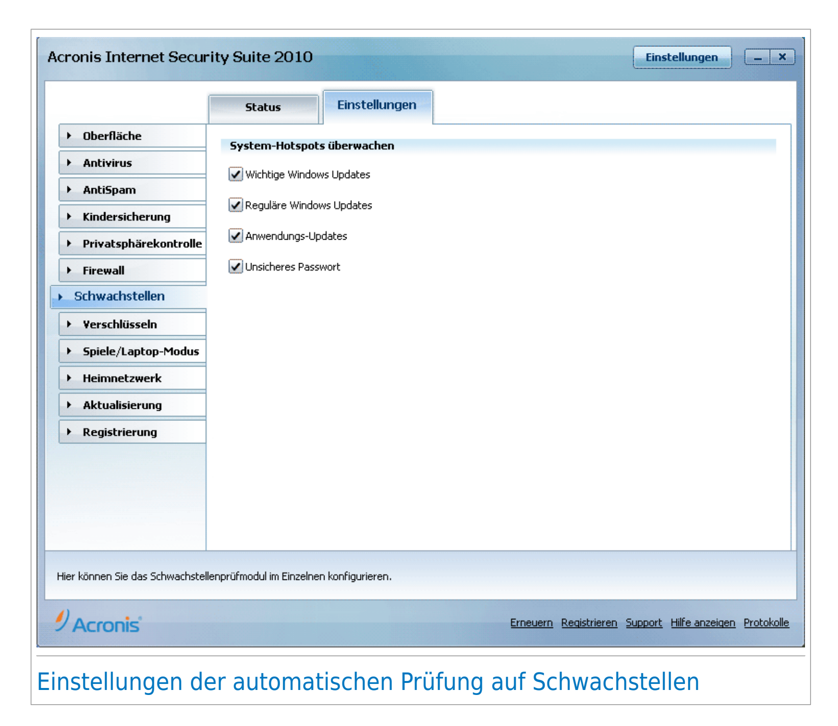
Abhängig vom Problem, um eine spezifische Schwachstelle zu beheben, gehen Sie folgendermaßen vor:

- Wenn Windows Updates verfügbar sind, klicken Sie auf **Installieren** in die **Action** Leiste um diese zu installieren.
- Wenn eine Anwendung nicht auf dem neusten Stand ist, Nutzen Sie den auf der Webseite **verfügbaren**) Link um die aktuellste Version herunterzuladen und zu installieren.
- Falls ein Windowskonto ein schwaches Passwort hat,klicken Sie auf **Beheben** und fordern Sie den Benutzer beim nächsten Windows-Login auf, das Passwort zu ändern oder ändern Sie es selbst. Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (so wie #, $ or @).

Um Ihren Computer auf Schwachstellen zu prüfen, klicken Sie auf **Jetzt prüfen** und folgen Sie den Schritten des Assistenten um die Schwachstellen zu beheben. Für weitere Informationen lesen Sie bitte *„Schwachstellenprüfassistent“* (S. 56).

22.2. Einstellungen

Um die Einstellungen für die automatische Prüfung auf Schwachstellen zu verwalten, klicken Sie auf **Schwachstellen>Einstellungen** in der Profiansicht.



Einstellungen der automatischen Prüfung auf Schwachstellen

Markieren Sie die Kontrollkästchen der entsprechenden Systemschwachstellen die regelmäßig überprüft werden sollen.

- **Wichtige Windows Updates**
- **Normale Windows Updates**
- **Anwendungs-Updates**
- **Unsichere Passwörter**



Anmerkung

Wenn Sie das Kontrollkästchen für eine bestimmte Schwachstelle freilassen, wird Acronis Internet Security Suite 2010 Sie nicht über die entsprechenden Probleme und Risiken informieren.

23. Verschlüsseln

Acronis Internet Security Suite 2010 bietet Verschlüsselungsmöglichkeiten um Ihre vertraulichen Dokumente und Ihre Unterhaltungen über Instant Messaging mit dem Yahoo Messenger und dem MSN Messenger zu schützen.

23.1. Instant Messaging (IM) Verschlüsselung

Acronis Internet Security Suite 2010 verschlüsselt standardmäßig alle Ihre Unterhaltungen über IM-Chats, vorausgesetzt dass:

- Ihr Gesprächspartner hat ein Acronis-Produkt installiert, das verschlüsselte Instant-Messaging-Übertragungen unterstützt und diese Verschlüsselung beim für das Gespräch verwendeten Instant Messaging-Programm aktiviert wurde.
- Sie und Ihr Chatpartner verwenden entweder Yahoo Messenger oder Windows Live (MSN) Messenger.

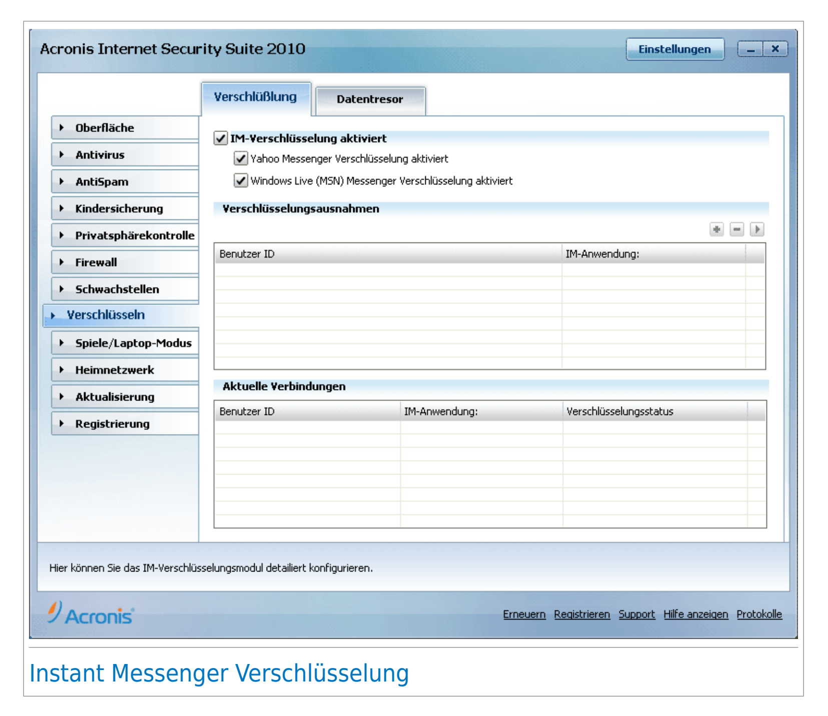


Wichtig
Acronis Internet Security Suite 2010 verschlüsselt die Unterhaltung nicht, wenn ein Chatpartner eine webbasierte Chat-Anwendung verwendet, so wie Meebo, oder eine andere Anwendung die Yahoo Messenger oder Windows Live (MSN) Messenger unterstützt.

Um die IM-Verschlüsselung zu konfigurieren klicken Sie auf **Verschlüsselung>IM-Verschlüsselung** in der Profiansicht.



Anmerkung
Sie können die IM-Verschlüsselung einfach mit der Acronis Toolbar von dem Chat-Fenster aus konfigurieren. Für weitere Informationen lesen Sie bitte *„Integration in Instant Messenger Programme“* (S. 276).



Instant Messenger Verschlüsselung

Die IM-Verschlüsselung ist standardmäßig für Yahoo Messenger und Windows Live (MSN) Messenger aktiviert. Sie können die IM-Verschlüsselung für eine bestimmte Anwendung oder komplett deaktivieren.

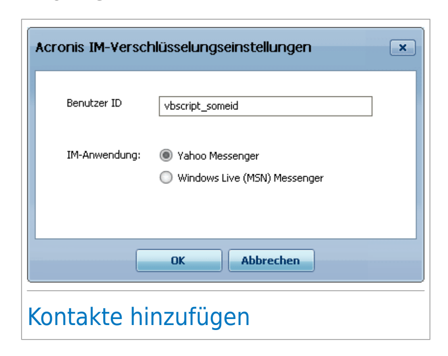
Zwei Tabellen werden angezeigt:

- **Verschlüsselungsausnahmen** - listet die Benutzer-IDs und das entsprechende IM-Programm auf, für den die Verschlüsselung deaktiviert ist. Um einen Kontakt aus der Liste zu entfernen, wählen Sie ihn aus und klicken Sie auf die Schaltfläche ⊟ **Entfernen**.
- **Aktuelle Verbindungen** - listet die aktuellen Instant Messaging Verbindungen auf (Benutzer ID und entsprechendes IM-Programm) und zeigt an, ob diese verschlüsselt sind oder nicht. Eine Verbindung kann aus folgenden Gründen nicht verschlüsselt sein:
  - Sie haben die Verschlüsselung für den entsprechenden Kontakt deaktiviert.
  - Ihr Kontakt hat kein Acronis-Produkt installiert, das eine Instant Messaging-Verschlüsselung unterstützt.

23.1.1. Verschlüsselung für bestimmte Benutzer deaktivieren

Um die Verschlüsselung für einen bestimmten Benutzer zu deaktivieren, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf die Schaltfläche **Hinzufügen** um das Konfigurationsfenster zu öffnen.



Kontakte hinzufügen

2. Geben Sie die Benutzer-ID Ihres Kontaktes in das Editierfeld ein.
3. Wählen Sie die Chat-Anwendung des Kontaktes.
4. Klicken Sie auf **OK**.

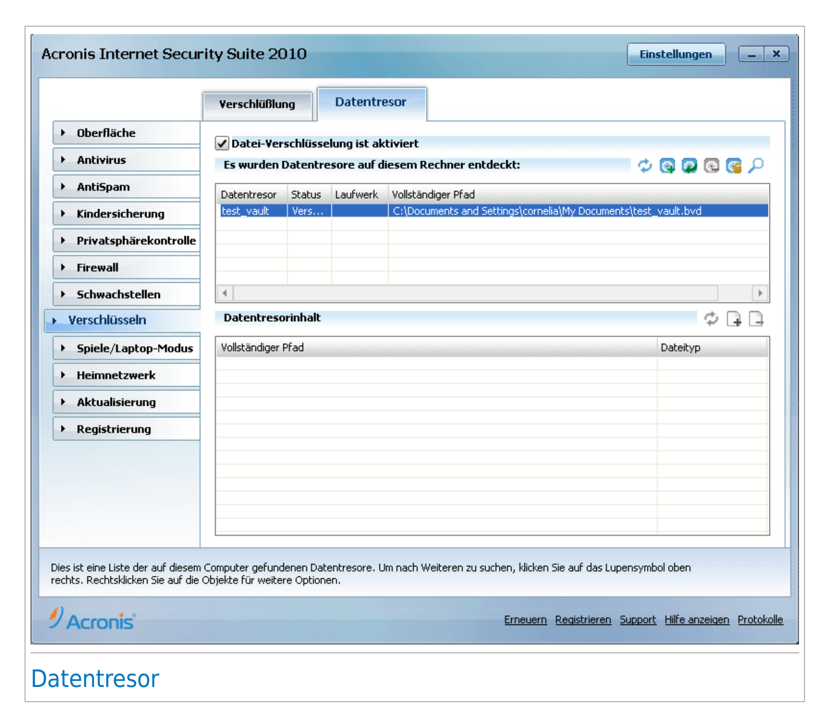
23.2. Datei

Der Verschlüsselung gibt Ihnen die Möglichkeit verschlüsselte, passwortgeschützte logische Laufwerke (oder einen Schutz) auf Ihrem Computer zu erstellen, in denen Sie sicher Ihre wichtigen und vertraulichen Daten speichern können. Die Daten, die im Schutz gespeichert sind, können nur von der Person gesehen werden, die das Passwort kennt.

Mit dem Passwort können Sie einen Schutz öffnen, Daten speichern und den Schutz abschließen, wobei dieser sicher bleibt. Wenn ein Schutz geöffnet ist, können Sie neue Dateien hinzufügen, auf aktuelle Dateien zugreifen oder diese verändern.

Der Dateischutz ist eine verschlüsselte Datei auf Ihrer Festplatte mit der Endung bvd. Auch wenn die Dateien, die den Dateischutz darstellen von anderen Betriebssystemen gelesen werden können, (beispielsweise Linux), können die sich darin befindenen Informationen nicht gelesen werden, weil sie verschlüsselt sind.

Um den Datentresor auf Ihrem Computer zu verwalten klicken Sie auf **Verschlüsselung>Dateiverschlüsselung** in der Profiansicht.



Datentresor

Um den Datentresor zu deaktivieren, lassen Sie das Kontrollkästchen **Verschlüsselung ist aktiviert** frei und klicken Sie auf **Ja** um zu bestätigen. Wenn Sie den Dateischutz deaktivieren, wird jeder Dateischutz abgeschlossen und Sie haben keinen Zugriff mehr auf die sich darin befindenden Dateien.

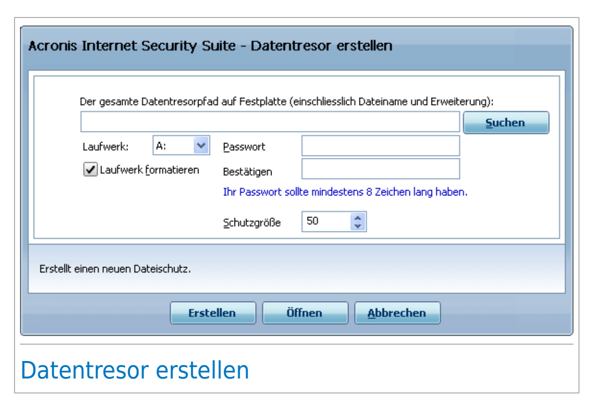
Die obere Tabelle zeigt den Dateischutz auf Ihrem Computer an. Sie können den Namen, den Status (offen/geschlossen), den Laufwerkbuchstaben und den vollständigen Pfad des Schutzes sehen. Die untere Tabelle zeigt den Inhalt des ausgewählten Schutzes an.

23.2.1. Einen Dateischutz erstellen

Um einen Dateischutz zu erstellen verwenden Sie eine der folgenden Methoden:

- Klicken Sie auf **Schutz erstellen**.
- Klicken Sie mit der rechten Maustaste auf die Schutztabelle und wählen Sie **Erstellen**.
- Klicken Sie mit der rechten Maustaste auf Ihren Desktop oder in einem Ordner auf Ihrem Computer, wählen Sie **Acronis Internet Security Suite Dateischutz** und wählen Sie dann **Erstellen**.

Ein neues Fenster wird sich öffnen.



Datentresor erstellen

Gehen Sie wie folgt vor:

1. Geben Sie den Speicherort und den Namen des Dateischutzes an.
   - Klicken Sie auf **Durchsuchen** um den gewünschten Speicherort auszuwählen und den Dateischutz unter dem gewünschten Namen zu speichern.
   - Um einen Tresor unter Arbeitsplatz zu erstellen, tragen Sie einfach den Namen des Tresors in das entsprechende Feld ein. Um Meine Dokumente zu öffnen, klicken Sie auf start Windows Start Menu und dann **Meine Dokumente**.
   - Geben Sie den vollen Pfad des Dateischutzes auf der Festplatte ein. Zum Beispiel `C:\my_vault.bvd`.
2. Wählen Sie einen Laufwerkbuchstaben aus dem Menu. Wenn Sie einen Schutz öffnen, wird ein virtuelles Laufwerk mit dem gewählten Laufwerkbuchstaben unter Arbeitsplatz erscheinen.
3. Geben Sie das neue Passwort des Tresors in die Felder **Neues Passwort** und **Neues Passwort bestätigen** ein. Jeder, der den Schutz öffnen und auf die Dateien zugreifen möchte muss zuerst das Passwort angeben.
4. Wählen **Laufwerk formatieren** um das virtuelle Laufwerk des Dateischutzes zu formatieren. Sie müssen das Laufwerk formatieren bevor Sie Daten in den Tresor hinzufügen können.
5. Wenn Sie die Standardgröße (50 MB) des Schutzes ändern möchten geben Sie den gewünschten Wert in das Feld **Schutzgröße** ein.
6. Klicken Sie auf **Erstellen** wenn Sie den Schutz unter dem gewünschten Speicherort ersetllen möchten. Um den Schutz als ein virtuelles Laufwerk unter Arbeitsplatz zu erstellen und anzuzeigen, klicken Sie auf **Erstelen&Öffnen**

Acronis Internet Security Suite 2010 wird Sie unmittelbar über das Ergebnis der Operation informieren. Falls ein Fehler auftaucht, verwenden Sie die Meldung um den Fehler zu untersuchen. Klicken Sie auf **OK**, um dieses Fenster zu schließen.



Anmerkung

Es ist praktischer alle Datentresore am gleichen Ort zu speichern. Auf diese Art sind Sie einfacher zu finden.

23.2.2. Einen Schutz öffnen

Um auf die Dateien in einem Schutz zugreifen und mit ihnen arbeiten zu können, muss der Schutz geöffnet werden. Wenn Sie einen Schutz öffnen, erscheint ein virtuelles Laufwerk unter Arbeitsplatz. Das Laufwerk hat den Laufwerkbuchstaben, der dem Schutz zugewiesen wurde.

Um einen Schutz zu öffnen verwenden Sie bitte folgende Methoden:

- Wählen Sie den Schutz aus der Tabelle und klicken Sie auf **Schutz öffnen**.
- Klicken Sie mit der rechten Maustaste auf den Schutz in der Tabelle und wählen Sie **Öffnen**.
- Klicken Sie mit der rechten Maustaste auf den Dateischutz unter Arbeitsplatz, gehen Sie auf **Acronis Internet Security Suite Dateischutz** und wählen Sie **Öffnen**.

Ein neues Fenster wird sich öffnen.



Dateischutz öffnen

Gehen Sie wie folgt vor:

1. Wählen Sie einen Laufwerkbuchstaben aus dem Menu.
2. Geben Sie das Schutz-Passwort in das Feld **Passwort** ein.
3. Klicken Sie auf **Öffnen**.

Acronis Internet Security Suite 2010 wird Sie unmittelbar über das Ergebnis der Operation informieren. Falls ein Fehler auftaucht, verwenden Sie die Meldung um den Fehler zu untersuchen. Klicken Sie auf **OK**, um dieses Fenster zu schließen.

23.2.3. Schutz abschließen

Wenn Sie mit Ihrer Arbeit im Schutz fertig sind, müssen Sie diesen abschließen um Ihre Daten zu schützen. Duch das Verschliessen des Tresors, verschwindet das entsprechende virtuelle Laufwerk aus dem Arbeitsplatz. Infolgedessen ist der Zugriff auf die sich im Tresor befindlichen Daten vollständig blockiert.

Um den Dateischutz abzuschließen verwenden Sie bitte folgende Methoden:

- Wählen Sie den Schutz aus der Tabelle und klicken Sie auf **Schutz abschließen**.
- Klicken Sie mit der rechten Maustaste auf den Schutz in der Tabelle und wählen Sie **Abschließen**.
- Klicken Sie mit der rechten Maustaste auf das entsprechende virtuelle Laufwerk unter Arbeitsplatz, gehen Sie auf **Acronis Internet Security Suite Dateischutz** und wählen Sie **Abschließen**.

Acronis Internet Security Suite 2010 wird Sie unmittelbar über das Ergebnis der Operation informieren. Falls ein Fehler auftaucht, verwenden Sie die Meldung um den Fehler zu untersuchen. Klicken Sie auf **OK**, um dieses Fenster zu schließen.

23.2.4. Passwort für Schutz ändern

Der Tresor muss verschlossen sein bevor man sein Passwort ändern kann. Um das Passwort für einen Schutz zu ändern, verwenden Sie bitte folgende Methoden:

- Wählen Sie den Schutz aus der Tabelle und klicken Sie auf **Passwort ändern**.
- Klicken Sie mit der rechten Maustaste auf den Schutz in der Tabelle und wählen Sie **Passwort ändern**.
- Klicken Sie mit der rechten Maustaste auf den Dateischutz unter Arbeitsplatz, gehen Sie auf **Acronis Internet Security Suite Dateischutz** und wählen Sie **Passwort ändern**.

Ein neues Fenster wird sich öffnen.



Passwort für Schutz ändern

Gehen Sie wie folgt vor:

1. Geben Sie das aktuelle Passwort des Schutzes in das Feld **Altes Passwort** ein.
2. Geben Sie das neue Passwort des Schutzes in die Felder **Neues Passwort** und **Neues Passwort bestätigen** ein.



Anmerkung

Ihr Passwort muss mindestens 8 Zeichen lang sein. Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (so wie #, $ or @).

3. Klicken Sie auf **OK**, um das Passwort zu ändern.

Acronis Internet Security Suite 2010 wird Sie unmittelbar über das Ergebnis der Operation informieren. Falls ein Fehler auftaucht, verwenden Sie die Meldung um den Fehler zu untersuchen. Klicken Sie auf **OK**, um dieses Fenster zu schließen.

23.2.5. Dateien zu einem Schutz hinzufügen

Um Dateien zu einem Schutz hinzuzufügen, befolgen Sie folgende Schritte:

1. Wählen Sie aus der Tabelle den Tresor aus zu welchem Sie Dateien hinzufügen möchten.
2. Falls der Tresor verschlossen ist, müssen Sie ihn zunächst öffnen (Rechtklick auf den Tresor und wählen Sie **Öffne Tresor**).
3. Klicken Sie auf **Datei hinzufügen**. Ein neues Fenster wird sich öffnen.
4. Wählen Sie welche Dateien / Ordner zum Schutz hinzugefügt werden sollen.
5. Klicken Sie auf **OK** um die ausgewählten Objekte in den Schutz zu kopieren.

Sobald der Tresor offen ist, können Sie des entsprechende virtuelle Laufwerk benutzen. Folgen Sie diesen Schritten:

1. Öffnen Sie den Arbeitsplatz, klicken Sie start Windows Start Menu und dann auf **Arbeitsplatz**).
2. Geben Sie das virtuelle Laufwerk entsprechend dem Tresor an. Sehen Sie nach dem von Ihnen festgelegten Laufwerksbuchstaben wenn Sie den Tresor öffnen möchten.
3. Kopieren/Ausschneiden oder drag&drop Dateien und Ordner direkt zu diesem virtuellen Laufwerk.

23.2.6. Dateien aus einem Schutz entfernen

Um eine Datei aus einem Schutz zu entfernen, befolgen Sie folgende Schritte:

1. Wählen Sie aus der Schutztabelle den Schutz, der die Dateien enthält, die Sie entfernen möchten.
2. Falls der Tresor verschlossen ist, müssen Sie ihn zunächst öffnen (Rechtklick auf den Tresor und wählen Sie **Öffne Tresor**).
3. Wählen Sie die zu entfernende Datei aus der Tabelle, die den Schutzinhalt anzeigt.
4. Klicken Sie **Lösche Dateien/Ordner**.

Wenn der Schutz geöffnet ist, können Sie Dateien direkt aus dem virtuellen Laufwerk, dem der Schutz zugewiesen ist, entfernen. Folgen Sie diesen Schritten:

1. Öffnen Sie den Arbeitsplatz, klicken Sie start Windows Start Menu und dann auf **Arbeitsplatz**).
2. Geben Sie das virtuelle Laufwerk entsprechend dem Tresor an. Sehen Sie nach dem von Ihnen festgelegten Laufwerksbuchstaben wenn Sie den Tresor öffnen möchten.
3. Entfernen Sie Dateien oder Ordner wie Sie es normalerweise auch in Windows tun (z.B. rechtsklicken Sie eine Datei die Sie löschen möchten und wählen sie **Löschen**)aus.

24. Spiele-/Laptop-Modus

Das Modul Spiele-/Laptop-Modus gibt ihnen die Möglichkeit spezielle Betriebsmodi von Acronis Internet Security Suite 2010 zu konfigurieren.

- Der Spiele-Modus verändert die Schutzeinstellungen zeitweise derart, dass ihr Einfluss auf die Leistungsfähigkeit des Systems während Sie spielen so gering wie möglich ist.
- Der Laptop-Modus stoppt voreingestellte Aufgaben wenn der Laptop über einen Akku betrieben wird, um dessen Laufzeit zu verlängern.

24.1. Spiele-Modus

Der Spiele-Modus ändert die Schutzeinstellungen zeitweise, dass ihr Einfluss auf die Leistungsfähigkeit des Systems so gering wie möglich ist. Wenn Sie den Spiele-Modus aktivieren, werden folgende Einstellungen angewendet:

- Alle Acronis Internet Security Suite 2010 Alarme und Pop-ups werden deaktiviert.
- Der Echtzeit-Schutz wird auf **Tolerant** gestellt.
- Die Acronis Internet Security Suite 2010 Firewall ist auf**Alle erlauben** eingestellt. Das bedeutet, dass alle neuen Verbindungen (eingehend und ausgehend) automatisch erlaubt werden, unabhängig vom verwendeten Port oder Protokoll.
- Updates werden nicht standardmäßig durchgeführt.



Anmerkung

Um diese Einstellung zu ändern, gehen Sie zu Update>Einstellungen und lassen Sie das Kontrollkästchen **Kein Update im Spiele-Modus** frei.

- Voreingestellte Prüfaufgaben sind standardmäßig deaktiviert.

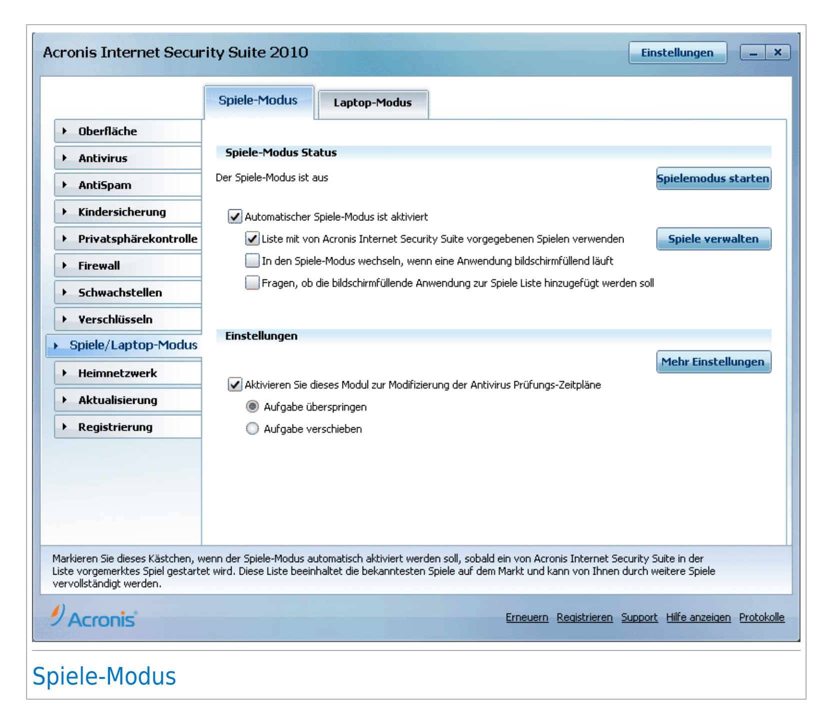
Standardmäßig wechselt Acronis Internet Security Suite 2010 automatisch in den Spielemodus, wenn Sie ein Spiel aus der Liste bekannter Spiele starten oder wenn eine Anwendung in die Vollbilddarstellung geht. Mit dem Tastenkürzel `Strg+Alt+Shift+G` können Sie den Spiele-Modus manuell starten. Es wird dringend empfohlen dass Sie den Spiele-Modus verlassen, wenn Sie mit dem Spielen fertig sind (Sie können dafür das selbe Tastenkürzel verwenden `Ctrl+Alt+Shift+G`).



Anmerkung

Wenn der Spiele-Modus aktiviert ist, sehen Sie den Buchstaben G über dem Acronis Symbol.

Um den Spiele-Modus zu konfigurieren klicken Sie auf **Spiele / Laptop Modus>Spiele-Modus** in der Profiansicht.



Spiele-Modus

Im oberen Bereich des Abschnitts können Sie den Status des Spiele-Modus sehen. Sie können auf**Spiele-Modus starten** oder **Spiele-Modus beenden** klicken um den aktuellen Status zu verändern.

24.1.1. Automatischen Spiele-Modus konfigurieren

Im automatischen Spiele-Modus kann Acronis Internet Security Suite 2010 selbtständig den Spiele-Modus starten, wenn ein Spiel entdeckt wird. Folgende Optionen können konfiguriert werden:

- **Liste mit von Acronis Internet Security Suite vorgegebenen Spielen verwenden** - damit Acronis Internet Security Suite 2010 automatisch in den Spiele-Modus wechselt, wenn Sie ein in der Liste aufgeführtes Spiel starten. Um diese Liste zu sehen, klicken Sie auf **Spiele verwalten** und dann **Erlaubte Spiele ansehen**.
- **Spiele-Modus bei Vollbild starten** - wenn eine Anwendung auf dem gesamten Bildschirm ausgeführt wird startet der Spiele-Modus automatisch.
- **Anwendung zur Spieleliste hinzufügen?** - um aufgefordert zu werden, eine neue Anwendung zur Spieleliste hinzuzufügen wenn Sie das Vollbild verlassen. Indem Sie eine neue Anwendung zur Spieleliste hinzufügen, wird Acronis Internet

Security Suite 2010 den Spiele-Modus automatisch starten, wenn Sie diese Anwendung das nächste Mal starten.

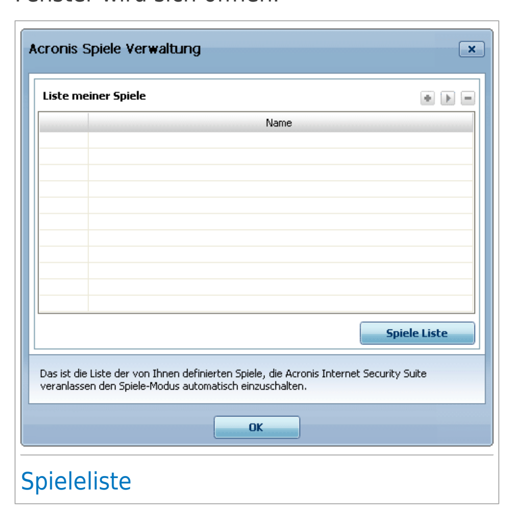


Anmerkung

Wenn Sie nicht möchten, dass Acronis Internet Security Suite 2010 den Spiele-Modus automatisch startet, lassen Sie das Kontrollkästchen **Automatischer Spiele-Modus** frei.

24.1.2. Spieleliste verwalten

Acronis Internet Security Suite 2010 startet den Spiele-Modus automatisch, wenn eine Anwendung gestartet wird die sich auf der Spiele-Liste befindet. Um die Spieleliste zu sehen und zu verwalten, klicken Sie auf**Spiele verwalten**. Ein neues Fenster wird sich öffnen.



Spieleliste

Neue Anwendungen werden automatisch zur Liste hinzugefügt, wenn:

- Sie ein Spiel starten das Acronis Internet Security Suite 2010 bekannt ist. Um diese Liste zu sehen, klicken Sie auf **Erlaubte Spiele betrachten**.
- Nachdem Sie das Vollbild beendet haben, können Sie das Spiel über das Aufforderungsfenster zur Spieleliste hinzufügen.

Wenn Sie den automatischen Spiele-Modus für eine bestimmte Anwendung von der Liste deaktivieren möchten, lassen Sie das entsprechende Kontrollkästchen frei. Sie sollten den automatischen Spiele-Modus für reguläre Anwendungen die den gesamten Bildschirm verwenden deaktiviert lassen, so wie Web-Browser und Mediaplayer.

Um die Spiele-Liste zu verwalten, können Sie die Schaltflächen verwenden, die sich im oberen Bereich der Tabelle befineden:

- Klicken Sie auf **Hinzufügen** um eine neue Anwendung zu der Spieleliste hinzufügen.
- **Entfernen** - dient zum Entfernen einer Anwendung von der Spieleliste.
- Klicken Sie auf **OK** um den Eintrag aus der Spieleliste zu editieren.

Spiele hinzufügen oder bearbeiten

Wenn Sie einen Eintag der Spiele-Liste hinzufügen oder bearbeiten, wird folgendes Fenster erscheinen:



Spiel hinzufügen

Klicken Sie auf **Durchsuchen** um die Anwendung auszuwählen oder geben Sie den vollständigen Pfad der Anwendung in das Editierfeld ein.

Wenn Sie nicht möchten, dass der Spiele-Modus automatisch startet, wenn eine bestimmte Anwendung gestartet wird, wählen Sie **Deaktivieren**.

Klicken Sie auf **OK** um den Eintrag zu der Spieleliste hinzuzufügen.

24.1.3. Einstellungen des Spiele-Modus konfigurieren

Um das Verhalten voreingestellter Aufgaben zu konfigurieren, verwenden Sie diese Optionen:

- **Dieses Modul aktivieren, um geplante Antivirus-Prüfaufgaben zu bearbeiten** - um zu verhindern, dass geplante Prüfaufgaben starten, während der Spiele-Modus aktiviert ist. Folgende Optionen sind wählbar:

Optionen	Beschreibung
Aufgabe überspringen	Die voreingestellte Aufgabe wird überhaupt nicht ausgeführt.

Optionen	Beschreibung
Aufgabe verschieben	Die geplante Aufgabe wird sofort ausgeführt, wenn der Spiele-Modus beendet wird.

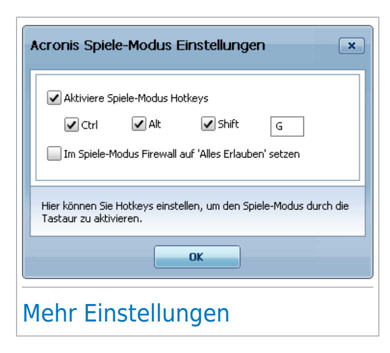
Um die Acronis Internet Security Suite 2010 Firewall automatisch zu deaktivieren, wenn der Spiele-Modus ausgeführt wird, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **Weitere Einstellungen**. Ein neues Fenster wird sich öffnen.
2. Wählen Sie **Alle Erlauben (Spiele-Modus)**.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

24.1.4. Tastenkombination für Spiele-Modus ändern

Mit dem Tastenkürzel `Strg+Alt+Shift+G` können Sie den Spiele-Modus manuell starten. Wenn Sie die Tastenkombination ändern möchten, befolgen Sie folgende Schritte:

1. Klicken Sie auf **Weitere Einstellungen**. Ein neues Fenster wird sich öffnen.



Mehr Einstellungen

2. Wählen Sie die gewünschte Tastenkombination unter der Option **Tastenkombination aktivieren** :
   - Wählen Sie die Tastenkombination die Sie verwenden möchten indem Sie folgende Tasten markieren : Steuerung (`Strg`), Shift (`Shift`) oder Alt-Taste (`Alt`).
   - Geben Sie im Editierfeld die Taste ein, die Sie benutzen möchten.

   Wenn Sie beispielsweise die Tastenkombination `Strg+Alt+D` benutzen möchten, markieren Sie `Strg` und `Alt` und geben Sie `D` ein.



Anmerkung

Wenn Sie die Markierung neben **Tastenkombination** entfernen, wird die Tastenkombination deaktiviert.

3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

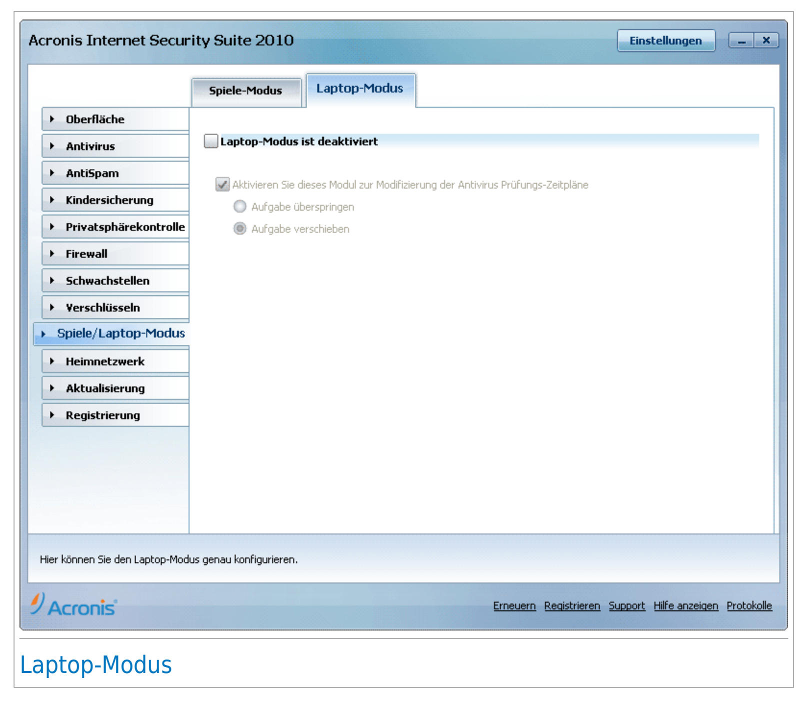
24.2. Laptop-Modus

Der 'Laptop-Modus' wurde speziell für Laptop- und Notebook-Benutzer entwickelt. Sein Zweck liegt darin, den Einfluss von Acronis Internet Security Suite 2010 auf den Stromverbrauch bei Batteriebetrieb zu minimieren.

Während der Laptop-Modus ausgeführt wird, werden voreingestellte Aufgaben standardmäßig nicht durchgeführt.

Acronis Internet Security Suite 2010 erkennt wenn Ihr Laptop über ein Akku läuft und startet den Laptop-Modus automatisch. Ebenso beendet Acronis Internet Security Suite 2010 automatisch den Laptop-Modus, wenn erkannt wird dass der Laptop nicht mehr über einen Akku betrieben wird.

Um den Laptop-Modus zu konfigurieren klicken Sie auf **Spiele / Laptop Modus>Laptop-Modus** in der Profiansicht.



Laptop-Modus

Sie können sehen ob der Laptop-Modus aktiviert ist oder nicht. Ist der Laptop-Modus aktiviert, wird Acronis Internet Security Suite 2010 die konfigurierten Einstellungen anwenden, wenn der Laptop über einen Akku betrieben wird.

24.2.1. Einstellungen des Laptop-Modus konfigurieren

Um das Verhalten voreingestellter Aufgaben zu konfigurieren, verwenden Sie diese Optionen:

- **Dieses Modul aktivieren, um geplante Antivirus-Prüfaufgaben zu bearbeiten** - um zu verhindern dass geplante Prüfaufgaben starten, während der Laptopmodus aktiviert ist. Folgende Optionen sind wählbar:

Optionen	Beschreibung
Aufgabe überspringen	Die voreingestellte Aufgabe wird überhaupt nicht ausgeführt.
Aufgabe verschieben	Die Aufgabe wird sofort durchgeführt, sobald der Laptop-Modus beendet wird.

25. Heimnetzwerk

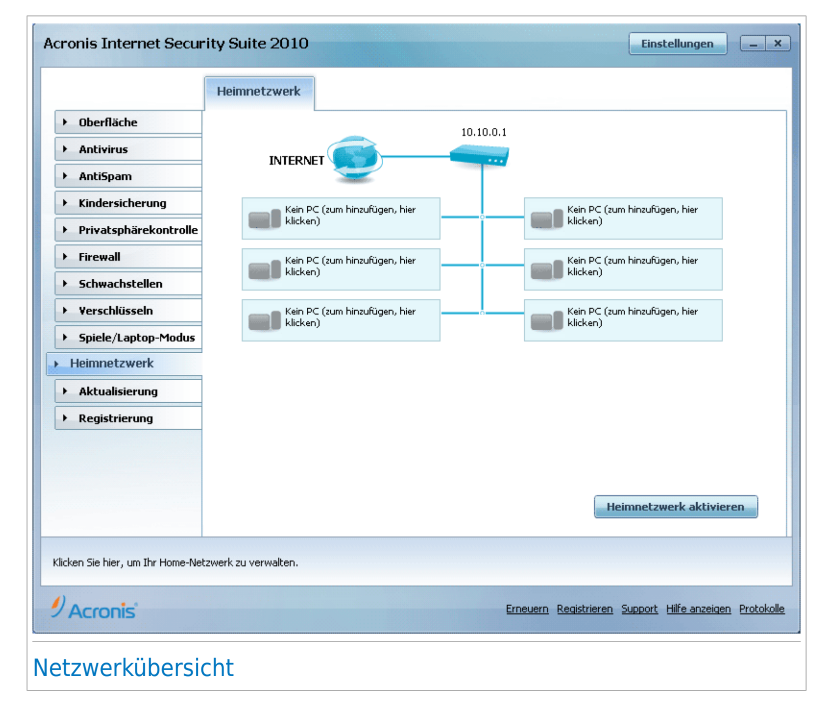
Mit dem Netzwerk-Modul können Sie die Acronis Produkte die auf den Computern in Ihrem Haushalt installiert sind von einem Computer aus verwalten.



Wichtig

Sie können nur die folgenden Acronis Sicherheitsprodukte verwalten:

- Acronis AntiVirus 2010
- Acronis Internet Security Suite 2010
- Acronis Backup and Security 2010



Netzwerkübersicht

Um die Acronis Produkte, die auf den Computern in Ihrem Haushalt installiert sind verwalten zu können, befolgen Sie diese Schritte:

1. Fügen Sie Ihren Computer dem Acronis Home-Netzwerk hinzu. Das Hinzufügen zu einem Netzwerk besteht aus dem Konfigurieren eines administrativen Passworts für die Verwaltung des Home-Netzwerks.

2. Fügen Sie jeden Computer, den Sie verwalten möchten dem Home-Netzwerk hinzu (Passwort einstellen).

3. Fügen Sie die Computer die Sie verwalten möchten ebenfalls auf Ihrem Computer hinzu.

25.1. Dem Acronis-Netzwerk beitreten

Um dem Acronis Home-Netzwerk beizutreten, befolgen Sie diese Schritte:

1. Klicken Sie **Netzwerk aktivieren**. Sie werden dazu aufgefordert, das Passwort für die Home-Verwaltung zu konfigurieren.



Passwort konfigurieren

2. Geben Sie das selbe Passwort in jedes der Editierfelder ein.
3. Klicken Sie auf **OK**.

Sie sehen den Namen des Computers in der Netzwerkübersicht.

25.2. Computer zum Acronis-Netzwerk hinzufügen

Um einen Computer zum Acronis Home-Netzwerk hinzuzufügen, müssen Sie zuerst das Passwort der Acronis Home-Verwaltung auf dem entsprechenden Computer konfigurieren.

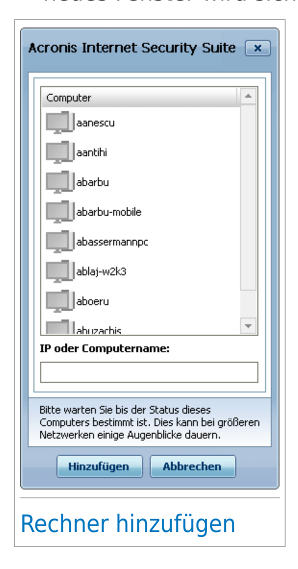
Um einen Computer zum Acronis Home-Netzwerk hinzuzufügen, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **PC hinzufügen**. Sie werden dazu aufgefordert, das Passwort für die lokale Home-Verwaltung anzugeben.



Passwort eingeben

2. Geben Sie das Passwort für die Home-Verwaltung ein und klicken Sie auf **OK**. Ein neues Fenster wird sich öffnen.



Rechner hinzufügen

Sie können eine Liste der Computer im Netzwerk sehen. Die Bedeutung des Symbols ist wie folgt:

Verdeutlicht einen online befindlichen Computer, auf dem kein verwaltbares Acronis-Produkt installiert ist.

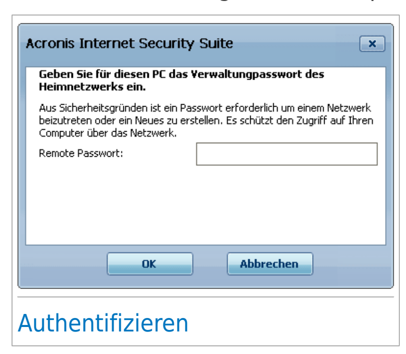
Verdeutlicht einen online befindlichen Computer, auf dem ein verwaltbares Acronis-Produkt installiert ist.

Verdeutlicht einen offline befindlichen Computer, auf dem ein verwaltbares Acronis-Produkt installiert ist.

3. Sie können hierzu eine der folgenden Methoden wählen:

- Wählen Sie aus der Liste den Namen des Computers der hinzugefügt werden soll:
- Geben Sie die IP-Adresse oder den Namen des Computers, der hinzugefügt werden soll in das dafür vorgesehene Feld ein.

4. Klicken Sie auf **Hinzufügen**. Sie werden dazu aufgefordert, das Passwort der Home-Verwaltung für den entsprechenden Computer einzugeben.



Authentifizieren

5. Geben Sie das Passwort für die Home-Verwaltung ein, das auf dem entsprechenden Computer konfiguriert wurde.
6. Klicken Sie auf **OK**. Wenn Sie das korrekt Passwort angegeben haben, wird der ausgewählte Computername in der Netzwerkübersicht erscheinen.

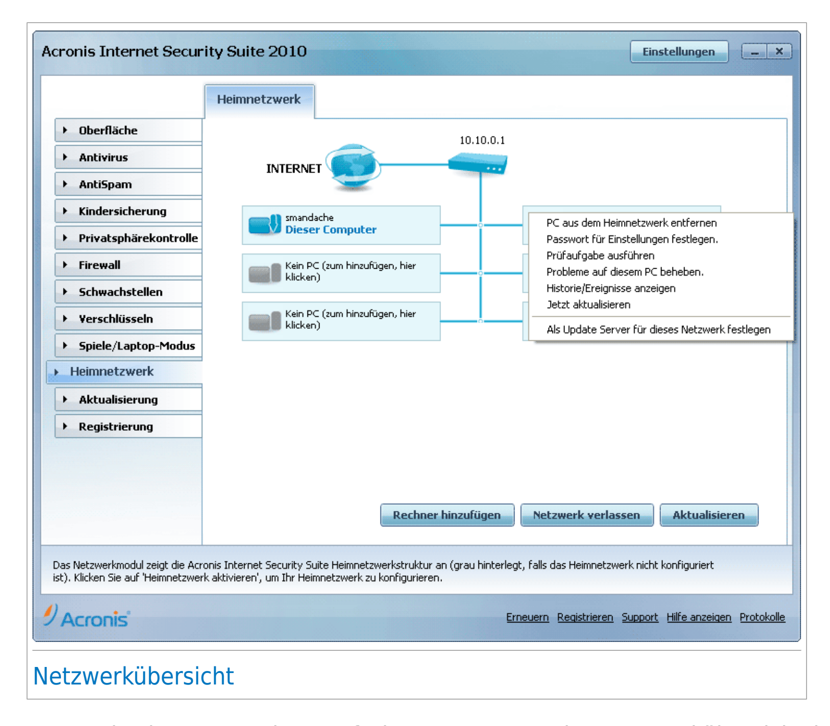


Anmerkung

Sie können bis zu fünf Computern zu der Netzwerkübersicht hinzufügen.

25.3. Das Acronis-Netzwerk verwalten

Wenn Sie das Acronis Home-Netzwerk erstellt haben, können Sie alle Acronis Produkte von einem Computer aus verwalten.



Netzwerkübersicht

Wenn Sie den Mauszeiger auf einen Computer der Netzwerkübersicht bewegen, können Sie einige Informationen über diesen sehen (Name, IP-Adresse, Anzahl der Probleme die die Systemsicherheit betreffen).

Wenn Sie mit der rechten Mautaste auf einen Computernamen im Netzwerk klicken, können Sie alle administrativen Aufgaben sehen, die Sie auf dem Remote-Computer ausführen können.

- **Aus diesem Netzwerk entfernen**

  Erlaubt Ihnen einen Pc aus dem Netzwerk entfernen.

- **Passwort für Einstellungen festlegen**

  Erlaubt Ihnen einen Passwort zu erstellen um den Zugang zu den Acronis Einstellungen auf diesem PC einschränken.

- **On-Demand Prüfaufgabe starten**

  Lässt sie eine On-Demand Prüfung auf dem Remote-PC durchführen. Sie können jede der folgenden Prüfungen tätigen: Meine Dokumente- System-, oder tiefgehende System-Prüfung.

- **Alle Probleme auf diesem PC beheben**

Lässt Sie alle Risiken die die Sicherheit Ihres Systems gefährden beheben, indem Sie dem Alle Risiken beheben Assistenten folgen.

- **Historie anzeigen/Ereignisse**

  Erlaubt den Zugriff auf das **Historie&Ereignisse** Modul des auf diesem PC installierten Acronis Produkts.

- **Jetzt aktualisieren**

  Initialisiert das Updateprozess für das Acronis Produkt das auf diesen Computer installiert ist.

- **Kindersicherung Einstellungen**

  Erlaubt es die Alterskategorie festzulegen welche vom Kindersicherungs-Webfilter auf diesem PC verwendet werden soll: Kind, Jugendlicher oder Erwachsener.

- **Diesen Computer als Update-Server für dieses Netzwerk festlegen**

  Erlaubt Ihnen diesen Rechner als Update-Server einzurichten, für alle Rechner aus dem Netzwerk, wo Acronis installiert ist. Unter Verwendung dieser Option, wird der Internetverkehr verringert, weil nur ein Rechner aus dem Netzwerk sich an das Internet anschließt um die Updates herunterzuladen.

Bevor Sie eine Aufgabe auf einem bestimmten Computer ausführen können, werden Sie dazu aufgefordert das Passwort der lokalen Home-Verwaltung anzugeben.



Passwort eingeben

Geben Sie das Passwort für die Home-Verwaltung ein und klicken Sie auf **OK**.



Anmerkung

Wenn Sie mehrere Aufgaben durchführen möchten, dann wählen Sie **In dieser Sitzung nicht nochmals fragen**. Wenn Sie diese Option wählen, werden Sie während der laufenden Sitzung nicht nochmals nach einem Passwort gefragt.

26. Aktualisierung

Jeden Tag werden neue Viren entdeckt und identifiziert. Aus diesem Grund ist es von großer Bedeutung, dass Sie das Programm Acronis Internet Security Suite 2010 stets mit den neuesten Virensignaturen betreiben.

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung verfügen, arbeitet Acronis Internet Security Suite 2010 eigenständig. Es prüft beim Start des Computers, ob neue Virensignaturen verfügbar sind und prüft nach Bedarf anschliessend jede **Stunde** nach Updates.

Wenn ein Update entdeckt wird, können Sie um eine Bestätigung für das Update gebeten werden oder das Update wird automatisch durchgeführt, je nach den Einstellungen für das automatische Update.

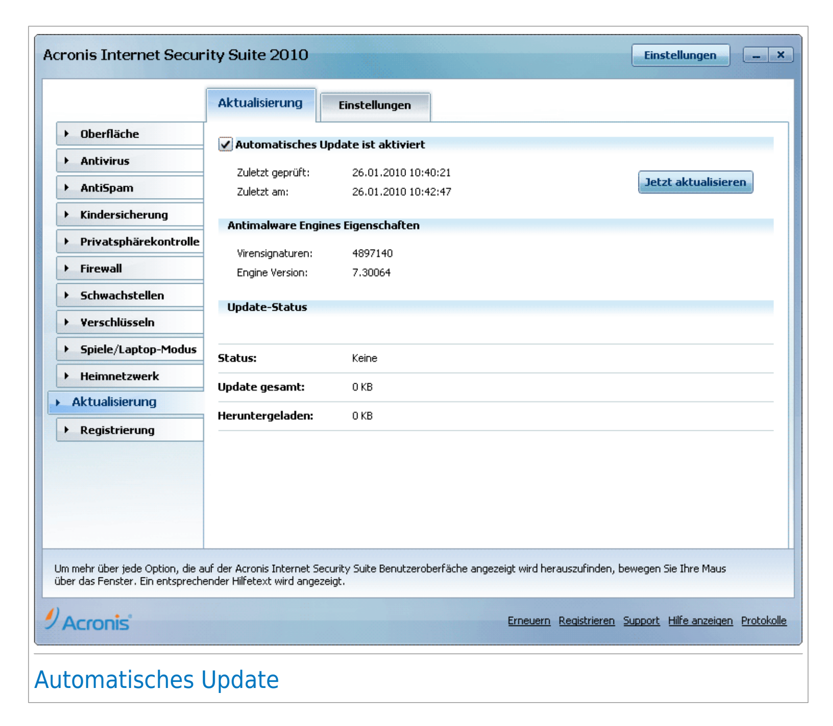
Der Updatevorgang wird "on the fly" durchgeführt, das bedeutet die entsprechenden Dateien stufenweise geupdated werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System wird nicht gefährdet.

Folgende Update-Möglichkeiten stehen zur Verfügung:

- **Updates für die AntiViren-Schutz** - Täglich gibt es neue Bedrohungen für Ihren PC. Daher müssen die Virendefinitionen stets auf den neusten Stand gebracht werden. Diesen Vorgang nennt man **Virendefinitions-Update**.
- **Updates für die Antispam Prüfung** - Um den Spamschutz zu verbessern, werden neue Regeln zur Heuristik und zum URL-Filter hinzugefügt. Diesen Vorgang nennt man **Antispam-Update**.
- **Updates für die AntiSpyware Prüfung** - Neue Spyware Signaturen werden kontinuierlich zur BitDefender Datenbank hinzugefügt. Diesen Vorgang nennt man **AntiSpyware-Update**.
- **Produkt-Update** - Wenn eine neue Version von BitDefender erscheint, mit neuen Funktionen und Erkennungstechniken, die eine Verbesserung der Such- und Erkennungsleistung mit sich bringt. Diesen Vorgang nennt man **Produkt-Update**.

26.1. Automatisches Update

Um Informationen zum Update zu erhalten und automatische Updates auszuführen, klicken Sie auf **Update>Update** in der Profiansicht.



Automatisches Update

Hier können Sie sehen wann das letzte Update durchgeführt wurde und wann zuletzt eine Prüfung nach Update stattgefunden hat. (und ob das Update erfolgreich war) Ausserdem werden Informationen zur momentanen Engineversion und zur Virensignatur angezeigt.

Wenn Sie das Updatemodul während eines Updates öffnen können Sie den aktuellen Status in Echtzeit einsehen.



Wichtig
Um den Schutz vor Spyware aus dem Internet zu gewährleisten, halten Sie Ihre **Automatisches Update** Funktion jederzeit aktiviert.

26.1.1. Benutzergesteuertes Update

Das automatische Update kann auch jederzeit über den Klick **Prüfen** erfolgen. Diese Funktion wird auch als **benutzergesteuertes Update** bezeichnet.

Das **Update** Modul verbindet Ihren Computer automatisch mit dem Acronis Update Server und benachrichtigt Sie bei einem verfügbaren Update. Wenn ein neues Update verfügbar ist, wird je nach vorgenommener Einstellung entweder abgefragt ob das Update erfolgen soll, oder das Update erfolgt automatisch.



Wichtig

Möglicherweise kann ein Neustart nach dem vollständig durchgeführten Update notwendig werden. Wir empfehlen Ihnen, den Neustart möglichst bald durchzuführen.



Anmerkung

Falls Sie über eine Internetverbindung per Einwahl verfügen, ist es sinnvoll, regelmäßig ein manuelles Acronis Internet Security Suite 2010-Update durchzuführen.

26.1.2. Automatisches Update deaktivieren

Wenn Sie das Automatische Update deaktivieren erscheint ein Warnfenster. Sie müssen Ihre Einstellung bestätigen indem Sie definieren wie lange das Automatisch Update deaktiviert werden soll. Zur Verfügung stehen die Optionen 5, 15 oder 30 Minuten, eine Stunde, permanent oder bis zum nächsten Systemstart.



Warnung

Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen die Deaktivierungszeit so gering wie möglich zu halten da Acronis Internet Security Suite 2010 Sie nur gegen die neusten Bedrohungen schützen kann wenn dieser aktuell ist.

26.2. Update-Einstellungen

Updates können vom lokalen Netz, über das Internet, direkt oder durch einen Proxy-Server durchgeführt werden. Standardmässig prüft Acronis Internet Security Suite 2010 jede Stunde auf neue Updates und installiert diese ohne Ihr zutun.

Um Updateeinstellungen vorzunehmen und Proxys zu konfigurieren klicken auf **Update>Einstellungen** in der Profiansicht.



Update-Einstellungen

Das Fenster mit den Update-Einstellungen enthält vier aufklappbare Optionskategorien (**Update-Adresse**, **Einstellungen für das Automatische Update**, **Einstellungen für das manuelle Update** und **Weitere Einstellungen**). Jede Kategorie wird seperat beschrieben.

26.2.1. Update-Adresse

Um eine Update-Adresse festzulegen verwenden Sie die Optionen der **Update-Adresse** Kategorie.



Wichtig

Ändern Sie diese Einstellungen nur wenn Sie mit einem lokalen Updateserver verbunden sind oder wenn das Update über einen Proxy erfolgt.

Um die Update-Adresse zu ändern geben Sie die Adresse des lokalen Servers in das gewünschte **URL** Feld ein.



Anmerkung

Wir empfehlen den Primären Updateserver auf den lokalen Server zu ändern und den sekundären Server unverändert zu belassen sodass im Falle eines lokalen Serverausfalls dennoch Updates durchgeführt werden können.

Wenn Sie für den Zugang zum Internet einen Proxy verwenden, wählen Sie die Option **Proxy verwenden**, und klicken dann auf **Proxyverwaltung** um diese zu konfigurieren. Weitere Informationen finden Sie unter *„Proxyverwaltung“* (S. 262)

26.2.2. Automatisches Update konfigurieren

Um die Optionen des Automatischen Updates einzustellen verwenden Sie die Optionen unter **Einstellungen für das Automatische Update**.

Sie können die Anzahl der Stunden zwischen zwei aufeinander folgenden Updateprüfungen im Feld **Zeitinterval** festlegen. Standardmässig ist dieses auf eine Stunde eingestellt.

Um festzulegen wie das automatische Update durchgeführt werden soll können Sie zwischen den folgenden Optionen wählen:

- **Update im Hintergrund** - Acronis Internet Security Suite 2010 führt Updates komplett selbständig durch.
- **Nachfragen bevor Update heruntergeladen werden** - Immer wenn ein Update verfügbar ist werden Sie gefragt ob dieser heruntergeladen werden soll.
- **Nachfragen bevor Updates installiert werden** - BitDefender frägt den Benutzer bevor ein Update installiert wird.

26.2.3. Manuelle Update Einstellungen

Um festzulegen wie ein manuelles Update durchgeführt wird wählen Sie ein der folgenden Optionen in der Kategorie **Einstellungen für das manuelle Update**:

- **Stilles Update** - BitDefender führt Updates, ohne Benutzereingriff, komplett selbständig im Hintergrund durch.
- **Nachfragen bevor Update heruntergeladen werden** - Immer wenn ein Update verfügbar ist werden Sie gefragt ob dieser heruntergeladen werden soll.

26.2.4. Weitere Einstellungen konfigurieren

Um sicherzustellen das Sie bei der Arbeit nicht vom Updatevorgang gestört werden haben Sie folgende Optionen in der Kategorie **Weitere Einstellungen** zur Verfügung:

- **Auf Neustart warten, statt nachzufragen** - Wenn ein Update einen Neustart benötigt, wird das Produkt mit den alten Dateien weiterarbeiten, bis das System neu gebootet wird. Der Benutzer wird nicht zum Neustart aufgefordert, so dass der Update-Prozess von Acronis Internet Security Suite 2010 die Arbeit des Anwenders nicht beeinflusst.
- **Nicht aktualisieren wenn Prüfvorgang durchgeführt wird** - Acronis Internet Security Suite 2010 kann während des Prüfvorganges kein Update durchführen. Auf diese Weise kann der Update-Vorgang den Prüfvorgang nicht beeinflussen.



Anmerkung
Sollte Acronis Internet Security Suite 2010 während eines Prüfvorganges aktualisiert werden, wird der Prüfvorgang abgebrochen.

- **Nicht aktualisieren wenn der Spiele-Modus aktiv ist** - Wenn der Spiele-Modus aktiviert ist wird Acronis Internet Security Suite 2010 kein Update durchführen. Durch diese Option können Sie den Einfluss der Anwendung, auf die Geschindigkeit während des Spielens minimieren.

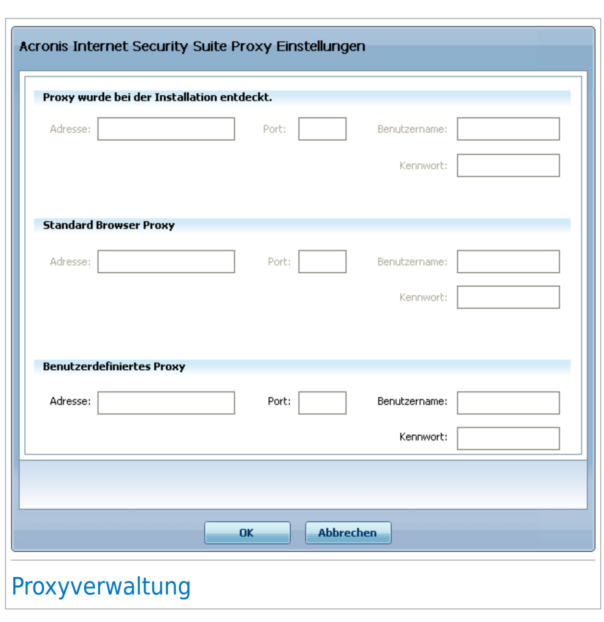
26.2.5. Proxyverwaltung

Falls Ihre Firma einen Proxy verwendet um eine Internetverbindung herzustellen müssen Sie diese in Acronis Internet Security Suite 2010 konfigurieren um sicherzustellen das ein Update möglich ist. Anderenfalls werden die Proxyeinstellungen des Administrators welcher das Produkt installiert hat, oder die momentanen Proxyeinstellungen des Standard-Browsers verwendet.



Anmerkung
Proxyeinstellungen können nur von Administratoren oder Hauptbenutzern (welche über das nötige Passwort verfügen) vorgenommen werden.

Um die Proxy-Einstellungen zu verwalten, klicken Sie **Proxy-Einstellungen**. Ein neues Fenster erscheint.



Proxyverwaltung

Es bestehen drei mögliche Proxyeinstellungen:

- **Proxy während Installation entdeckt** - Diese Einstellungen wurden zum Zeitpunkt der Installation von BitDefender erkannt. Diese können nur von eben diesem Administratorkonto verändert werden. Sollte ein Benutzername und Passwort nötig sein so geben Sie diesen in die dafür vorgesehenen Felder ein.
- **Standard Browser Proxy** - Proxy-Einstellungen des aktuellen Benutzers, extrahiert vom Standard-Browser. Falls der Proxy einen Benutzernamen und Passwort voraussetzt, geben Sie diese in den entsprechenden Feldern an.



Anmerkung

Die unterstützen Browser sind hierbei der Internet Explorer, Mozilla Firefox und Opera. Sollten Sie einen anderen Browser verwenden wird Acronis Internet Security Suite 2010 nicht in der Lage sein die Einstellungen zu übernehmen.

- **Benutzerdefinierte Proxy-Einstellungen** - Hier können Sie selbst, als Administrator eingeloggt, Proxyeinstellungen vornehmen .

  Die folgenden Einstellungen müssen angegeben werden:
  - **Adresse** - Geben Sie die IP-Adresse des Proxy-Servers ein.
  - **Port** - Geben Sie den Port ein, über den Acronis Internet Security Suite 2010 die Verbindung zum Proxy-Server herstellt.
  - **Name** - Geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
  - **Passwort** - Geben Sie das Passwort für den zuvor angegebenen Benutzer ein.

Bei einem Updateversuch werden alle Proxyeinstellung nacheinander verwendet bis ein Update möglich ist.

Zuerst wird versucht ein Update über die eigenen Proxyeinstellungen vorzunehmen. Als nächstes werden die Proxyeinstellungen des Administrators verwenden. Wenn auch dies nicht zum erfolgt führt wird ein Update über die Einstellungen des momentanen Benutzers durchgeführt.

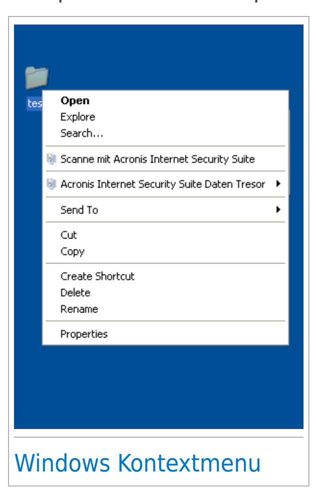
Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Klicken Sie auf **Übernehmen** um die Einstellungen zu speichern. Wenn Sie auf **Standard** klicken werden die Werkseinstellungen geladen.

Integration in Windows und Third-Party Software

27. Integration in das Windows Kontextmenu

Das Kontextmenu erscheint wann immer Sie eine Datei oder einen Ordner auf Ihrem Computer oder Desktop rechtsklicken.



Windows Kontextmenu

Acronis Internet Security Suite 2010 integriert sich in das Windows Kontextmenu um Ihnen beim leichten Prüfen von Dateien auf Viren zu helfen und andere Benutzer daran zu hindern auf Ihre sensiblen Dateien zuzugreifen. Sie können die Acronis Internet Security Suite 2010 Option im Kontextmenu schnell erkennen indem Sie nach dem Acronis Symbol schauen.

- Prüfe mit Acronis Internet Security Suite
- Acronis Internet Security Suite Datentresor

27.1. Scanne mit Acronis Internet Security Suite

Sie können das Kontextmenu verwenden um schnell und einfach Dateien, Ordner und sogar ganze Laufwerke prüfen zu lassen. Rechtsklicken Sie das zu prüfende Objekt und wählen Sie **Scanne mit Acronis Internet Security Suite** aus dem Menü aus. Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

Scanoptionen. Die Prüfoptionen sind für bestmögliche Enteckungsraten vorkonfiguriert. Falls infizierte Dateien entdeckt werden wird Acronis Internet Security Suite 2010 versuchen diese zu desinfizieren (den Mailwarecode entfernen). Wenn die Desinfizierung fehlschlagen sollte wird Ihnen der Antivirus Prüfassistent andere Möglichkeiten anbieten wie mit den infizierten Dateien verfahren werden kann.

Wenn Sie die Prüfoptionen ändern möchten, befolgen Sie die Schritte:

1. Öffnen Sie Acronis Internet Security Suite 2010 und wechseln Sie in die Profi-Ansicht.
2. Klicken Sie auf **Antivirus** in dem Menü auf der linken Seite.
3. Klicken Sie auf den Tab **Virenscan**
4. Rechtsklicken Sie die **Untermenuprüfung** und wählen Sie **Öffnen**. Ein neues Fenster wird sich öffnen.
5. Klicken Sie **Anpassen** und konfigurieren Sie die Prüfoption wie gewünscht. Um herauszufinden was eine Option macht, halten Sie den Mauszeiger darüber und lesen die angezeigte Beschreibung im unteren Teil des Fensters.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern.
7. Klicken Sie **OK** um die neue Prüfoption zu bestätigen und anzuwenden.



Wichtig

Sie sollten die Prüfoption dieser Prüfmethode nicht verändern, es sei den Sie haben einen triftigen Grund dazu.

27.2. Acronis Internet Security Suite Datentresor

Acronis Internet Security Suite Datentresor hilft Ihnen die vertraulichen Dokumente auf Ihrem Computer sicher aufzubewahren.

- Der Dateischutz ist ein sicherer Speicherplatz für persönliche Informationen oder sensible Dateien.
- Der Dateischutz ist eine verschlüsselte Datei auf Ihrem Computer mit der Endung bvd. Durch die Verschlüsselung sind die Daten innerhalb des Schutzes sicher vor Diebstahlversuchen oder Sicherheitsproblemen.
- Wenn Sie diesebvd Datei mounten, wird eine logische Partition (ein neues Laufwerk) erscheinen. Es wird leichter für Sie sein dieses Prozess zu verstehen, wenn Sie an einen ähnlichen denken: Ein ISO-Image als virtuelle CD zu mounten.

  Öffnen Sie einfach den Arbeitsplatz und Sie werden ein neues Laufwerk sehen, das den Dateischutz darstellt. Sie können Dateiprozesse (kopieren, löschen, ändern, usw) auf diesem Laufwerk durchführen. Die Dateien sind geschützt, solange sie sich in diesem Laufwerk befinden (denn für das Mounten ist ein Passwort notwendig).

  Wenn Sie fertig sind, schließen Sie Ihren Schutz ab (unmount) um dessen Inhalt zu schützen.

Sie können die Acronis Internet Security Suite 2010 Datentresore leicht auf Ihrem Rechner erkennen, durch das Acronis Symbol und die .bvd Erweiterung.



Anmerkung

Dieser Abschnitt zeigt Ihnen wie man einen Datentresor nur mit Hilfe der vom Windows Kontextmenu angebotenen Option einrichtet und verwaltet. Sie können Datentresore ebenso direkt in der Acronis Internet Security Suite 2010 Benutzeroberfläche erstellen und verwalten.

- Gehen Sie in der Mittleren Ansicht auf Datentresor Tab und verwenden Sie die Optionen des **Schnellmassnahmen**-Bereichs. Ein Assistent wird Ihnen helfen jede Aufgabe abzuschliessen.
- Für den direkteren Zugriff wechseln Sie in die Profi-Ansicht und klicken Sie **Verschlüsselung** im Menu auf der linken Seite. Im Datenverschlüsselung Tab, können Sie die existierenden Datentresore mitsamt ihrem Inhalt sehen und verwalten.

27.2.1. Schutz erstellen

Berücksichtigen Sie das ein Datentresor eigentlich nur eine Datei mit `.bvd` als Endung ist. Nur wenn Sie den Tresor öffnen erscheint im Arbeitsplatz ein virtuelles Laufwerk in welchem Sie leicht Dateien verstauen können. Wenn Sie einen Tresor erstellen müssen Sie festlegen wo und unter welchem Namen er zu speichern ist. Zudem muss ein Passwort zum Schutz des Inhalts bestimmt werden. Ausschliesslich Benutzer welchen das Passwort bekannt ist können den Tresor öffnen und auf die darin abgelegten Dokumente und Daten zugreifen.

Um einen Tresor zu erstellen, folgen Sie den Schritten:

1. Klicken Sie mit der rechten Maustaste auf Ihren Desktop oder in einem Ordner auf Ihrem Computer, wählen Sie **Acronis Internet Security Suite Datentresor** und wählen Sie dann **Datentresor erstellen**. Das folgende Fenster wird erscheinen:



Datentresor erstellen

2. Geben Sie den Speicherort und den Namen des Dateischutzes an.

- Klicken Sie auf **Durchsuchen** um den gewünschten Speicherort auszuwählen und den Dateischutz unter dem gewünschten Namen zu speichern.
- Um einen Tresor unter Arbeitsplatz zu erstellen, tragen Sie einfach den Namen des Tresors in das entsprechende Feld ein. Um Meine Dokumente zu öffnen, klicken Sie auf start Windows Start Menu und dann **Meine Dokumente**.
- Geben Sie den vollen Pfad des Dateischutzes auf der Festplatte ein. Zum Beispiel `C:\my_vault.bvd`.

3. Wählen Sie einen Laufwerkbuchstaben aus dem Menu. Wenn Sie einen Schutz öffnen, wird ein virtuelles Laufwerk mit dem gewählten Laufwerkbuchstaben unter Arbeitsplatz erscheinen.
4. Geben Sie das neue Passwort des Tresors in die Felder **Neues Passwort** und **Neues Passwort bestätigen** ein. Jeder, der den Schutz öffnen und auf die Dateien zugreifen möchte muss zuerst das Passwort angeben.
5. Wählen **Laufwerk formatieren** um das virtuelle Laufwerk des Dateischutzes zu formatieren. Sie müssen das Laufwerk formatieren bevor Sie Daten in den Tresor hinzufügen können.
6. Wenn Sie die Standardgröße (50 MB) des Schutzes ändern möchten geben Sie den gewünschten Wert in das Feld **Schutzgröße** ein.
7. Klicken Sie auf **Erstellen** wenn Sie den Schutz unter dem gewünschten Speicherort ersetllen möchten. Um den Schutz als ein virtuelles Laufwerk unter Arbeitsplatz zu erstellen und anzuzeigen, klicken Sie auf **Erstelen&Öffnen**

Acronis Internet Security Suite 2010 wird Sie unmittelbar über das Ergebnis der Operation informieren. Falls ein Fehler auftaucht, verwenden Sie die Meldung um den Fehler zu untersuchen. Klicken Sie auf **OK**, um dieses Fenster zu schließen.



Anmerkung
Es ist praktischer alle Datentresore am gleichen Ort zu speichern. Auf diese Art sind Sie einfacher zu finden.

27.2.2. Schutz öffnen

Um auf die Dateien in einem Schutz zugreifen und mit ihnen arbeiten zu können, muss der Schutz geöffnet werden. Wenn Sie einen Schutz öffnen, erscheint ein virtuelles Laufwerk unter Arbeitsplatz. Das Laufwerk hat den Laufwerkbuchstaben, der dem Schutz zugewiesen wurde.

Um einen Tresor zu öffnen befolgen Sie die Schritte:

1. Suchen Sie auf Ihrem Computer nach `.bvd` welches den Tresor representiert.
2. Rechtsklicken Sie die Datei, gehen Sie auf **Acronis Internet Security Suite Datentresor** und wählen Sie **Öffnen**. Die schnellere Alternative wäre die Datei

doppelt anzuklicken, oder rechtsklick und auswählen **Open**. Das folgende Fenster wird erscheinen:



Dateischutz öffnen

3. Wählen Sie einen Laufwerkbuchstaben aus dem Menu.
4. Geben Sie das Schutz-Passwort in das Feld **Passwort** ein.
5. Klicken Sie auf **Öffnen**.

Acronis Internet Security Suite 2010 wird Sie unmittelbar über das Ergebnis der Operation informieren. Falls ein Fehler auftaucht, verwenden Sie die Meldung um den Fehler zu untersuchen. Klicken Sie auf **OK**, um dieses Fenster zu schließen.

27.2.3. Schutz abschließen

Wenn Sie mit Ihrer Arbeit im Schutz fertig sind, müssen Sie diesen abschließen um Ihre Daten zu schützen. Duch das Verschliessen des Tresors, verschwindet das entsprechende virtuelle Laufwerk aus dem Arbeitsplatz. Infolgedessen ist der Zugriff auf die sich im Tresor befindlichen Daten vollständig blockiert.

Um einen Tresor zu schliessen, befolgen Sie die Schritte:

1. Öffnen Sie den Arbeitsplatz, klicken Sie start Windows Start Menu und dann auf **Arbeitsplatz**).
2. Ermitteln Sie das virtuelle Laufwerk welches dem Tresor entspricht den Sie zu schliessen wünschen. Sehen Sie nach dem von Ihnen festgelegten Laufwerksbuchstaben wenn Sie den Tresor öffnen möchten.
3. Rechtklicken Sie auf das dazugehörige Laufwerk, dann zu **Acronis Internet Security Suite Datentresor** und klicken Sie **Schliessen**.

Sie können auch einen Rechts-Klick auf die `.bvd` Datei machen, die den Datentresor repräsentiert, auf **Acronis Internet Security Suite Datentresor** zeigen und **Schliessen** klicken.

Acronis Internet Security Suite 2010 wird Sie unmittelbar über das Ergebnis der Operation informieren. Falls ein Fehler auftaucht, verwenden Sie die Meldung um den Fehler zu untersuchen. Klicken Sie auf **OK**, um dieses Fenster zu schließen.



Anmerkung

Wenn mehrere Tresore geöffnet sind, sollten Sie die Profiansicht des Acronis Internet Security Suite 2010s benutzen. Wenn Sie auf **Verschlüsselung**, Datentresor Tab gehen, sehen Sie eine Tabelle welche Ihnen Auskunft über die existierenden Tresore gibt. Diese Information enthält ob der Tresor geöffnet ist und, falls dem so ist, den Laufwerksbuchstaben der ihm zugeordnet wurde.

27.2.4. Dem Datentresor hinzufügen

Bevor Sie dem Tresor Dateien oder Ordner hinzufügen können müssen Sie den Tresor öffnen. Ist der Tresor ersteinmal geöffnet ist es ein Leichtes unter Verwendung des Kontextmenus darin Dateien oder Ordner zu lagern. Rechtsklicken Sie die Datei oder den Ordner welche Sie in den Tresor kopieren möchten, gehen Sie auf **Acronis Internet Security Suite Datentresor** und klicken Sie **dem Datentresor hinzufügen**.

- Wenn nur ein Datentresor geöffnet ist so wird die Datei oder Ordner direkt zu diesem kopiert.
- Falls mehrere Tresore geöffnet sind, werden Sie aufgefordert auszuwählen in welchen Tresor das Objekt kopiert werden soll. Wählen Sie aus dem Menu passend zum gewünschten Tresor den Laufwerksbuchstaben, und klicken Sie auf **OK** um das Objekt zu kopieren.

Sie können ebenso das entsprechende virtuelle Laufwerk auswählen. Folgen Sie diesen Schritten:

1. Öffnen Sie den Arbeitsplatz, klicken Sie start Windows Start Menu und dann auf **Arbeitsplatz**).
2. Geben Sie das virtuelle Laufwerk entsprechend dem Tresor an. Sehen Sie nach dem von Ihnen festgelegten Laufwerksbuchstaben wenn Sie den Tresor öffnen möchten.
3. Kopieren/Ausschneiden oder drag&drop Dateien und Ordner direkt zu diesem virtuellen Laufwerk.

27.2.5. Aus dem Datentresor entfernen

Um Datein oder Ordner aus dem Datentresor zu entfernen muss der Tresor geöffnet sein. Um Dateien oder Ordner aus dem Tresor zu entfernen, befolgen Sie diese Schritte:

1. Öffnen Sie den Arbeitsplatz, klicken Sie start Windows Start Menu und dann auf **Arbeitsplatz**).

2. Geben Sie das virtuelle Laufwerk entsprechend dem Tresor an. Sehen Sie nach dem von Ihnen festgelegten Laufwerksbuchstaben wenn Sie den Tresor öffnen möchten.
3. Entfernen Sie Dateien oder Ordner wie Sie es normalerweise auch in Windows tun (z.B. rechtsklicken Sie eine Datei die Sie löschen möchten und wählen sie **Löschen**)aus.

27.2.6. Passwort für Schutz ändern

Das Passwort schützt den Inhalt des Tresors vor unberechtigten Zugriffen. Ausschliesslich Benutzer welchen das Passwort bekannt ist können den Tresor öffnen und auf die darin abgelegten Dokumente und Daten zugreifen.

Der Tresor muss verschlossen sein bevor man sein Passwort ändern kann. Zum Ändern des Tresorspassworts, folgen Sie bitte den Schritten:

1. Suchen Sie auf Ihrem Computer nach `.bvd` welche den Tresor darstellt.
2. Rechtsklicken Sie die Datei, gehen Sie auf **Acronis Internet Security Suite Datentresor** und wählen Sie **Passwort ändern**. Das folgende Fenster wird erscheinen:



Passwort für Schutz ändern

3. Geben Sie das aktuelle Passwort des Datentresors in das Feld **Altes Passwort** ein.
4. Geben Sie das neue Passwort des Datentresors in die Felder **Neues Passwort** und **Neues Passwort bestätigen** ein.



Anmerkung

Ihr Passwort muss mindestens 8 Zeichen lang sein. Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (so wie #, $ or @).

5. Klicken Sie auf **OK**, um das Passwort zu ändern.

Acronis Internet Security Suite 2010 wird Sie unmittelbar über das Ergebnis der Operation informieren. Falls ein Fehler auftaucht, verwenden Sie die Meldung um den Fehler zu untersuchen. Klicken Sie auf **OK**, um dieses Fenster zu schließen.

28. Integration in Web-Browser

Acronis Internet Security Suite 2010 schützt Sie während des Surfens vor Phishingversuchen. Er prüft die Webseiten auf welche Sie zugreifen und warnt Sie vor Phishingseiten. Eine Whitelist von Webseiten welche nicht durch Acronis Internet Security Suite 2010 geprüft werden kann ebenfalls erstellt werden.

Acronis Internet Security Suite 2010 integriert sich über eine intuitive und einfach anzuwendende Toolbar in die folgenden Web-Browser:

- Internet Explorer
- Mozilla Firefox

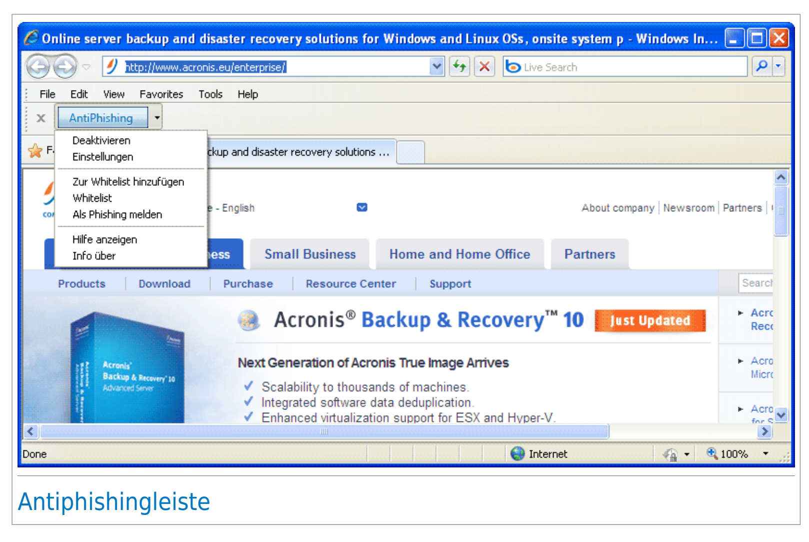
Sie können die Antiphishingeinstellungen und die Whitelist leicht und effizient über die Acronis Antiphishingleiste in den oben genannten Browsern verwalten.

Die Antiphishingleiste, symbolisiert durch das Acronis Icon, befindet sich im oberen Bereich des Browsers. Klicken Sie dieses an um die Leiste anzuzeigen.



Anmerkung

Sollten Sie die Leiste nicht sehen dann klicken Sie auf **Extras**, **Menüleiste** und wählen Sie **Acronis Leiste**.



Antiphishingleiste

Folgende Aktionen stehen in der Leiste zur Verfügung:

- **Aktivieren/Deaktivieren** - Aktiviert/deaktiviert die Acronis Internet Security Suite 2010 Antiphishingleiste im jetzigen Browser.

- **Einstellungen** - Öffnet ein Fenster in welchem Sie Einstellungen zur Antiphishingleiste vornehmen können. Die folgenden Optionen sind verfügbar:
  - **Echtzeit Antiphishing Webschutz** - entdeckt und warnt Sie in Echtzeit wenn eine Webseite "fischt" (also persönliche Informationen stiehlt). Diese Optionen steuert den Acronis Internet Security Suite 2010 Antiphishingschutz auschliesslich im derzeitigen Browser.
  - **Vor dem Hinzufügen zur Whitelist fragen** - Frägt Sie bevor eine Webseite zur Whitelist hinzugefügt wird.
- **Zu Whitelist hinzufügen** - Fügt die momentane Webseite zur Whitelist hinzu.



Anmerkung

Durch das hinzufügen zur Whitelist wird die Seite nicht mehr von Acronis Internet Security Suite 2010 auf Phishing geprüft. Wir empfehlen Ihnen nur Seiten hinzuzufügen welchen Sie vollständig vertrauen.

- **White List zeigen** - Öffnet die White List.



Antiphishing Whitelist

Sie können eine Liste der Webseiten sehen welche nicht von Acronis Internet Security Suite 2010 Antiphishing geprüft werden. Wenn Sie eine Webseite aus der Whitelist entfernen möchten, sodass die Webseite wieder auf Phishing geprüft wird, klicken Sie auf **Entfernen** neben dem gewünschten Eintrag.

Sie können Webseiten, welchen Sie vollständig vertrauen, zur Whitelist hinzufügen sodass diese nicht auf Phishing geprüft werden. Um eine Seite zur Whitelist hinzuzufügen geben Sie die Adresse in das entsprechende Feld ein und klicken Sie dann auf **Hinzufügen**.

- **Berichte Phishing** - informiert das Acronis Labor das Sie die fragliche Webseite in Betrat ziehen Datendiebstahl zu begehen. Durch berichten von phishing Webseiten helfen Sie andere leute gegen Datendiebstahl zu schützen.
- **Hilfe** - Öffnet die Hilfedatei.
- **Über** - Öffnet ein Fenster in welchem Sie Informationen über Acronis Internet Security Suite 2010 erhalten und Hilfe finden falls etwas unvorhergesehenes geschied.

29. Integration in Instant Messenger Programme

Acronis Internet Security Suite 2010 bietet Verschlüsselungsmöglichkeiten um Ihre vertraulichen Dokumente und Ihre Unterhaltungen über Instant Messaging mit dem Yahoo Messenger und dem MSN Messenger zu schützen.

Acronis Internet Security Suite 2010 verschlüsselt standardmäßig alle Ihre Unterhaltungen über IM-Chats, vorausgesetzt dass:

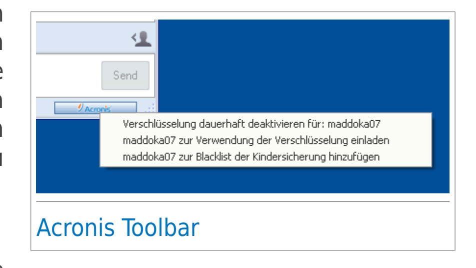
- Ihr Gesprächspartner hat ein Acronis-Produkt installiert, das verschlüsselte Instant-Messaging-Übertragungen unterstützt und diese Verschlüsselung beim für das Gespräch verwendeten Instant Messaging-Programm aktiviert wurde.
- Sie und Ihr Chatpartner verwenden entweder Yahoo Messenger oder Windows Live (MSN) Messenger.



Wichtig

Acronis Internet Security Suite 2010 verschlüsselt die Unterhaltung nicht, wenn ein Chatpartner eine webbasierte Chat-Anwendung verwendet, so wie Meebo, oder eine andere Anwendung die Yahoo Messenger oder Windows Live (MSN) Messenger unterstützt.

Sie können die IM-Verschlüsselung einfach mit der Acronis Toolbar von dem Chat-Fenster aus konfigurieren. Die Toolbar sollte sich in der unteren rechten Ecke des Chat-Fensters befinden. Sehen Sie nach dem Acronis Logo um sie zu finden.



Acronis Toolbar



Anmerkung

Die Toolbar zeigt eine verschlüsselte Konversation durch eine kleine Taste 🔑 direkt neben dem Acronis Logo an.

Durch klicken auf die Acronis Toolbar, erhalten Sie die folgenden Optionen:

- **Dauerhaft die Verschlüsselung für Kontakt deaktivieren.**
- **Einladen Kontakt Verschlüsselung zu verwenden.** Um Ihre Konversation zu verschlüsseln, muss auch das Gegenüber Acronis Internet Security Suite 2010 installiert haben und ein kompatibles IM Programm verwenden.
- **Kontakt zur Blacklist der Kindersicherung hinzufügen.** Wenn Sie den Kontakt zur Blacklist der Kindersicherung hinzufügen und diese aktiviert ist, so werden Sie keine weitere Nachricht von diesem Kontakt sehen. Um Kontakte aus der Blacklist zu entfernen klicken Sie in der Toolbar auf **Entfernencontact von der Blacklist der Kindersicherung**.

30. Integration in Mail Clients

Acronis Internet Security Suite 2010 enthält ein Antispam Modul. Antispam prüft E-Mails die Sie empfangen und spürt Spams auf. Spams die Acronis Internet Security Suite 2010 entdeckt, werden markiert dem [SPAM] Prefix in der Betreffzeile.



Anmerkung

Der Antispam-Schutz steht für alle POP3/SMTP E-Mail-Clients zur Verfügung.

Acronis Internet Security Suite 2010 integriert sich über eine intuitive und einfach anzuwendende Leisten in die folgenden Mail Clients:

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

Acronis Internet Security Suite 2010 legt Spam-Nachrichten automatisch in einem festgelegten Ordner ab, wie folgt:

- In Microsoft Outlook, Spams werden verschoben in den **Spam** Ordner, zu finden unter **gelöschte Objekte**. Der **Spam** Ordner wurde während der Installation von Acronis Internet Security Suite 2010 erstellt.
- In Outlook Express und Windows Mail, werden Spams direkt in **gelöschte Objekte** verschoben.
- Im Mozilla Thunderbird, werden Spams in den **Spam** Ordner verschoben, der unter **Trash** Ordner zu finden ist. Der **Spam** Ordner wurde während der Installation von Acronis Internet Security Suite 2010 erstellt.

Falls Sie andere E-Mail Clients verwenden, so müssen Sie eine Regel erstellen um Nachrichten die als [SPAM] markiert sind, in einen eigens erstellten Ordner zu verschieben.

30.1. Konfigurationsassistent

Beim ersten Start Ihres Mail-Clients nach der Installation von Acronis Internet Security Suite 2010 öffnet sich ein Assistent, der Sie dabei unterstützt, den Bayesian-Filter zu trainieren, sowie die Liste der Freunde und die Liste der Spammer zu konfigurieren, um die Effektivität der Antispamfilter zu erhöhen.



Anmerkung

Der Assistent kann jederzeit über die Schaltfläche **Assistent** in der Antispam-Toolbaraufgerufen werden.

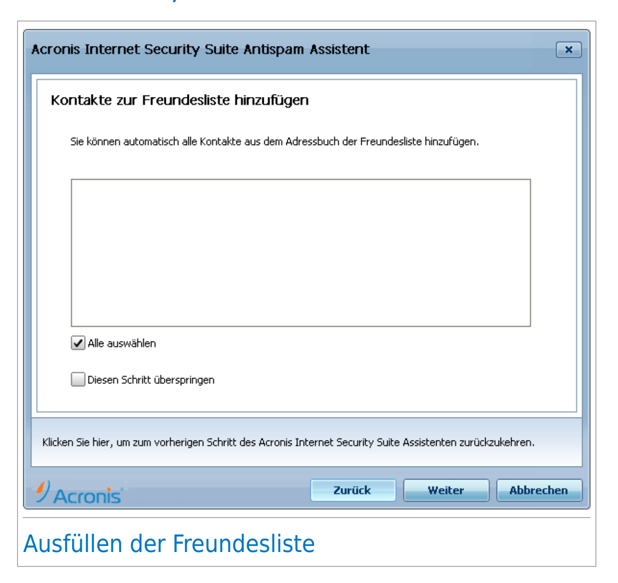
30.1.1. Schritt 1/6 - Einführung



Begrüßungsfenster

Klicken Sie auf **Weiter**.

30.1.2. Schritt 2/6 - Ausfüllen der Freundes-Liste



Ausfüllen der Freundesliste

Hier sehen Sie alle Ihre Adressen aus Ihrem **Adressbuch**. Bitte wählen Sie all die Adressen aus, die Sie Ihrer **Freundesliste** hinzufügen möchten (wir empfehlen Ihnen, alle zu markieren). Sie werden dann alle E-Mails von diesen Adressen erhalten, egal welchen Inhalts.

Um einen Kontakt zur Freundesliste hinzuzufügen klicken Sie auf **Alle auswählen**.

Wenn Sie diesen Bestätigungs Schritt überspringen möchten, wählt **Überspingen**. Klicken Sie auf **Weiter**.

30.1.3. Schritt 3/6 - Bayesianische Daten löschen



Bayesianische Daten löschen

Sie finden heraus, dass Ihr Antispam-Filter an Effektivität verloren hat. Dies kann daher kommen, dass das Training nicht genau durchgeführt worden ist (z. B. haben Sie versehentlich eine Anzahl legitimer Mails als Spam markiert oder umgekehrt). Falls Ihr Filter sehr ungenau arbeitet, müssen Sie Ihre Filterkriterien in Ihrer Datenbank löschen und neu anlegen. Dabei hilft Ihnen der Assistent.

Wählen Sie **Antispam Datenbank leeren**, wenn Sie die bayesianische Datenbank neu starten wollen.

Sie können die Bayesianische Datenbank in eine Datei speichern um Sie für andereAcronis Internet Security Suite 2010 Produkte oder nach einer Neuinstallation zu verwenden. Um die Trainingsdatenbank des bayesischen Filters zu speichern klicken Sie den Button **Bayes speichern** und wählen Sie den gewünschten Speicherort. Die Datei wird `.dat` als Erweiterung haben.

Um eine gsicherte Bayesianische Datenbank zu laden, wählen Sie **Loade Bayes** und öffnen die entsprechende Datei.

Wenn Sie diesen Bestätigungs Schritt überspringen möchten, wählt **Überspingen**. Klicken Sie auf **Weiter**.

30.1.4. Schritt 4/6 -Trainieren des Bayesian-Filters mit legitimen E-Mails



Trainieren des Bayesian-Filters mit legitimen E-Mails

Bitte wählen Sie einen Ordner, der legitime E-Mails enthält. Diese Nachrichten werden genutzt, um den Antispam Filter zu trainieren.

Es gibt zwei weitere Optionen unter der Ordnerliste:

- **Unterordner mit einbeziehen** - Um Unterordner in Ihre Auswahl zu übernehmen.
- **Automatisch zur Freundesliste hinzufügen** - Um den Sender zu der Liste der Freunde hinzuzufügen.

Wenn Sie diesen Bestätigungs Schritt überspringen möchten, wählt **Überspingen**. Klicken Sie auf **Weiter**.

30.1.5. Schritt 5/6 - Trainieren des Bayesian-Filters mit Spam-Mails



Trainieren des Bayesian-Filters mit Spam-Mails

Bitte wählen Sie einen Ordner, der Spam-E-Mails enthält. Diese Nachrichten werden genutzt, um den Antispam-Filter zu trainieren.



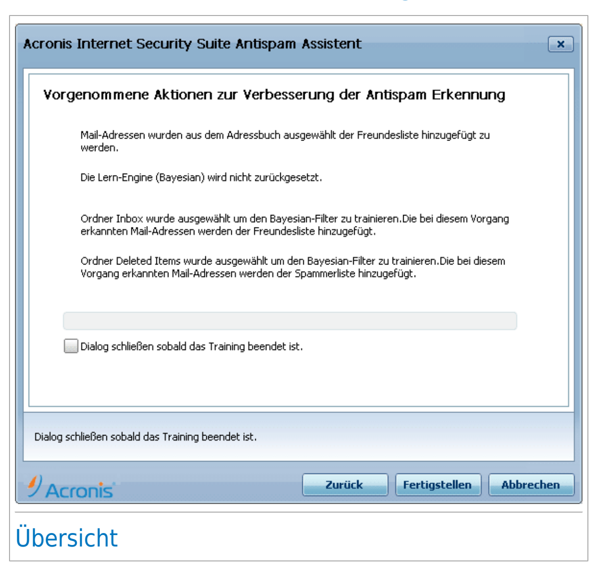
Wichtig
Bitte vergewissern Sie sich, dass der von Ihnen gewählte Ordner keine legitimen E-Mails enthält, ansonsten wird die Antispam-Leistung beträchtlich reduziert.

Es gibt zwei weitere Optionen unter der Ordnerliste:

- **Unterordner mit einbeziehen** - Um Unterordner in Ihre Auswahl zu übernehmen.
- **Automatisch zur Spamerliste hinzufügen** - Um den Sender zu der Liste der Spamer hinzuzufügen. E-Mail Nachrichten von diesem Sender werden immer als SPAM markiert und dementsprechend verarbeitet.

Wenn Sie diesen Bestätigungs Schritt überspringen möchten, wählt **Überspingen**. Klicken Sie auf **Weiter**.

30.1.6. Schritt 6/6 - Assistent abgeschlossen



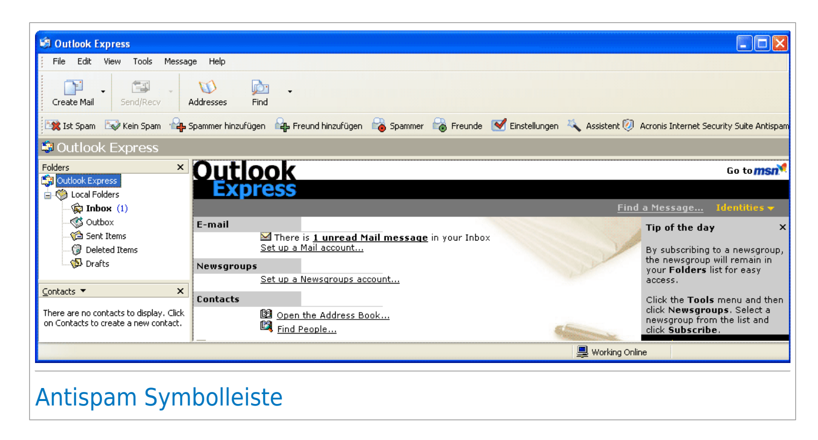
Übersicht

In diesem Fenster können Sie alle Einstellungen einsehen, die mit dem Konfigurationsassistenten durchgeführt worden sind. Sie können noch Änderungen vornehmen, indem Sie zum vorherigen Fenster zurückkehren (**Zurück**).

Wenn Sie keine Änderungen vornehmen wollen, klicken Sie auf **Fertigstellen**.

30.2. Antispam Symbolleiste

Im oberen Teil Ihres Mail Client Fensters können Sie die Antispamleiste sehen. Die Antispamleiste hilft Ihnen beim Verwalten des Antispamschutzes direkt vom E-Mail Client aus. Sie können Acronis Internet Security Suite 2010 ganz einfach korrigieren falls eine reguläre Mail als Spam markiert wurde.



Antispam Symbolleiste

Jede Schaltfläche der Symbolleiste von Acronis Internet Security Suite 2010 wird nachfolgend beschrieben:

- **Ist Spam** - Klicken Sie auf diesen Button und das bayesianische Modul erkennt die ausgewählten Mails als Spam. Sie werden als Spam markiert und in den **Spam**-Ordner verschoben.

  Zukünftige Mails mit diesem Muster werden alle als Spam markiert.

  ## Anmerkung
  Sie können eine oder mehrere E-Mails markieren.

- **Kein Spam** - teilt dem bayesianische Modul mit, daß die ausgewählte E-Mail kein Spam ist und Acronis Internet Security Suite 2010 sie nicht hätte markieren sollen. Die E-Mail wird aus dem **Spam** Ordner ins **Inbox** Ordner verschoben.

  Zukünftige E-Mails mit diesem Muster werden nicht mehr als Spam markiert.

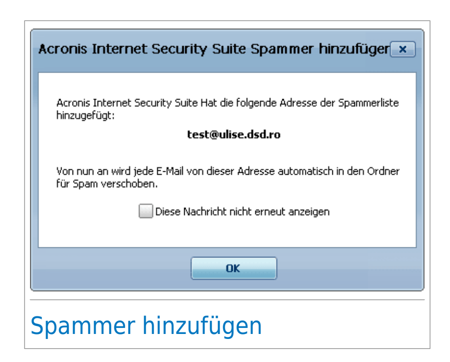
  

  ## Anmerkung
  Sie können eine oder mehrere E-Mails markieren.

  ## Wichtig
  Die Schaltfläche **Kein Spam** wird aktiv, wenn Sie eine Nachricht als Spam markiert haben (normalerweise werden diese Nachrichten in den **Spam**-Ordner verschoben).

- **Spammer hinzufügen** - fügt den Absender der ausgewählten E-Mail zur Liste der Spammer hinzu.



Spammer hinzufügen

Wählen Sie **Diese Nachricht nicht erneut anzeigen**, um dieses Fenster nicht mehr zu sehen, wenn Sie eine neue Spam-Mail in die Liste aufnehmen.

Klicken Sie auf **OK**, um dieses Fenster zu schließen.

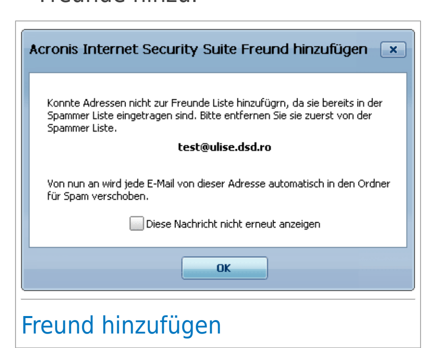
Zukünftige Mails mit diesem Muster werden nicht mehr als Spam markiert.



Anmerkung

Sie können einen oder mehrere Absender auswählen.

- **Freund hinzufügen** - fügt den Sender der ausgewählten E-Mail der Liste der Freunde hinzu.



Freund hinzufügen

Wählen Sie **Diese Nachricht nicht erneut anzeigen**, um dieses Fenster nicht mehr zu sehen, wenn Sie eine neue Freundesmail in die Liste aufnehmen.

Klicken Sie auf **OK**, um dieses Fenster zu schließen.

Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.



Anmerkung

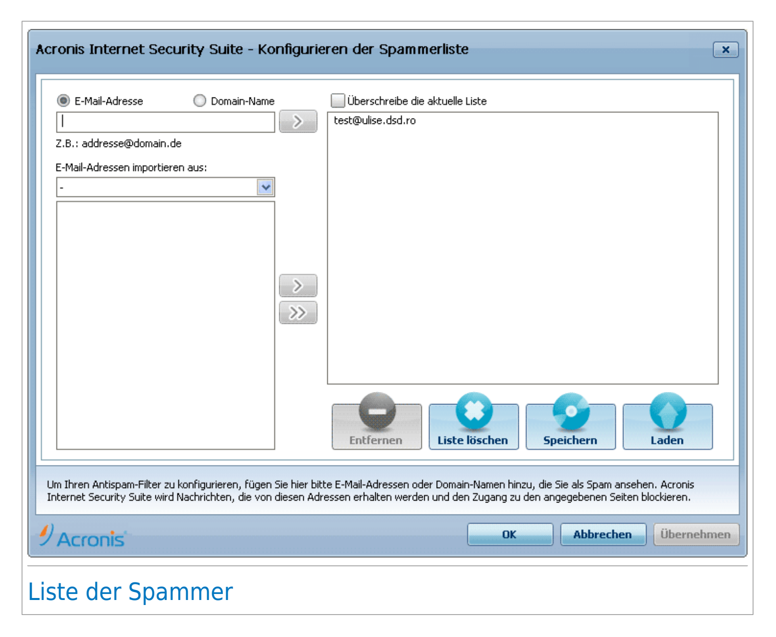
Sie können einen oder mehrere Absender auswählen.

- **Spammer** - Öffnen Sie **Spammerliste**. Sie enthält alle E-Mail-Adressen, von denen Sie keine Nachricht erhalten wollen, gleichwelchen Inhalts.



Anmerkung

Jede Mail von einer Adresse Ihrer **Spammerliste** wird automatisch in Ihren Papierkorb verschoben.



Liste der Spammer

Hier können Sie die Einträge Ihrer **Spammerliste** ändern.

Falls Sie eine E-Mail-Adresse hinzufügen möchten, kontrollieren Sie die **E-Mail-Adresse**, tragen Sie sie ein und klicken Sie auf den -Button. Die Adresse wird Ihrer **Spammerliste** hinzugefügt.



Wichtig

Syntax: name@domain.com.

Falls Sie eine Domain hinzufügen möchten, kontrollieren Sie sie und tragen Sie sie in das Feld **Domänen-Name** ein; klicken Sie auf den -Button. Die Domäne wird Ihrer **Spammerliste** hinzugefügt.



Wichtig

Syntax:

- @domain.com, *domain.com und domain.com - alle eingehenden Mails von domain.com werden als Spam markiert;
- *domain* - alle eingehenden Mails von domain (egal welcher Endung) werden als Spam markiert;
- *com - alle Mails mit dieser Endung com werden als Spam markiert.



Warnung

Fügen Sie keine legitime Webbasierte E-Mail Anbieter (wie: Yahoo, Gmail, Hotmail oder andere) zu der Spammerliste hinzu. Andernfalls werden die E-Mail-Nachrichten, die von jedem möglichem Benutzer solch eines Anbieters gesendet werden, als Spam eingestufft. z.B: wenn Sie `yahoo.com` zu Spammerliste hinzufügen, werden alle E-Mails die von `yahoo.com` Adressen kommen, als `[spam]` markiert.

Um E-Mail Adressen aus **Windows Addressenbuch** / **Outlook Express Pfade** in **Microsoft Outlook** / **Outlook Express** / **Windows Mail** zu impotieren, wählen Sie die adäqute Option aus **Importiere E-Mail Adressen aus** Menu.

Für **Microsoft Outlook Express** öffnet sich ein neues Fenster. Sie können nun den Ordner mit E-Mail Adressen auswählen, den Sie zur **Liste der Spammer** hinzufügen möchten. Klicken Sie anschließend auf **Auswählen**.

In beiden Fällen werden die E-Mail-Adressen in der Importliste erscheinen. Wählen Sie die gewünschten E-Mail-Adressen aus und klicken Sie auf den -Button, um sie zur **Spammerliste** hinzuzufügen. Wenn Sie anklicken, werden alle E-Mail-Adressen zur Spammerliste hinzugefügt.

Um einen Eintrag aus der Liste zu entfernen markieren Sie diesen und klicken Sie dann auf **Entfernen**. Um alle Einträge zu löschen, klicken Sie auf **Liste löschen** und danach auf **Ja** um dies zu bestätigen.

Sie können die Spammer Liste in eine Datei sichern, damit Sie sie nach einer Neuinstallation oder auf einem anderen Computer nutzen können. Um die Spammerliste zu speichern klicken Sie auf **Speichern** und speichern sie diese an den gewünschten Ort. Die Datei wird `.bwl` als Erweiterung haben.

Um eine zuvor gespeicherte Spammerliste zu laden, klicken Sie **Laden** und öffnen die entsprechende `.bwl` Datei. Um den Inhalt einer aktuellen Liste zurückzusetzen während der Inhalt einer zuvor gespeicherten Liste geladen wird, wählen Sie **Liste beim Laden leeren**.

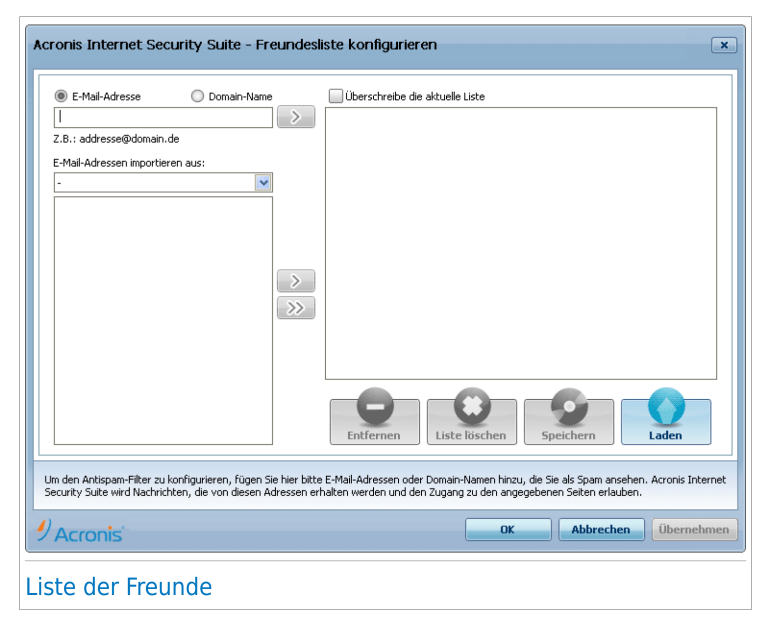
Klicken Sie auf **Übernehmen** und **OK**, um zu speichern und um die **Spammerliste** zu schließen.

- **Freunde** - Öffnen Sie **Freundenliste**. Sie enthält alle E-Mail-Adressen, von denen Sie immer Nachrichten erhalten wollen, gleichwelchen Inhalts.



Anmerkung

Jede Mail von einer Adresse Ihrer **Freundesliste** wird automatisch in Ihren Posteingang verschoben.



Liste der Freunde

Hier können Sie die Einträge Ihrer **Freundesliste** ändern.

Falls Sie eine E-Mail-Adresse hinzufügen möchten, kontrollieren Sie die **E-Mail-Adresse**, tragen Sie sie ein und klicken Sie auf den ⊡-Button. Die Adresse wird Ihrer **Spammerliste** hinzugefügt.



Wichtig

Syntax: name@domain.com.

Falls Sie eine Domain hinzufügen möchten, kontrollieren Sie diese und schreiben Sie sie in das Feld **Domänen-Name**; klicken Sie auf den ⊡-Button. Die Domain wird Ihrer **Freundesliste** hinzugefügt.



Wichtig

Syntax:

- @domain.com, *domain.com und domain.com - alle eingehenden Mails von domain.com werden in Ihren **Posteingang** verschoben, gleich welchen Inhalts;
- *domain* - alle eingehenden Mails von domain werden ohne Überprüfung Ihres Inhaltes in Ihren **Posteingang** verschoben, gleich welchen Inhalts;
- *com - alle Mails mit der Endung com werden in Ihren **Posteingang** verschoben, gleich welchen Inhalts;

Um E-Mail Adressen aus **Windows Addressenbuch** / **Outlook Express Pfade** in **Microsoft Outlook** / **Outlook Express** / **Windows Mail** zu impotieren, wählen Sie die adäqute Option aus **Importiere E-Mail Adressen aus** Menu.

Für **Microsoft Outlook Express** öffnet sich ein neues Fenster. Sie können nun den Ordner mit E-Mail Adressen auswählen, den Sie zur **Liste der Freunde** hinzufügen möchten. Klicken Sie anschließend auf **Auswählen**.

In beiden Fällen werden die E-Mail-Adressen in der Importliste erscheinen. Wählen Sie die gewünschten E-Mail-Adressen aus und klicken Sie auf den -Button, um sie zur **Freundesliste** hinzuzufügen. Wenn Sie anklicken, werden alle E-Mail-Adressen zur Freundesliste hinzugefügt.

Um einen Eintrag aus der Liste zu entfernen markieren Sie diesen und klicken Sie dann auf **Entfernen**. Um alle Einträge zu löschen, klicken Sie auf **Liste löschen** und danach auf **Ja** um dies zu bestätigen.

Sie können die Liste der Freunde speichern, so das diese auf einen anderen Rechner oder nach einer neuinstallation benutzt werden kann. Um die Freundesliste zu speichern klicken Sie auf **Speichern** und speichern sie diese an den gewünschten Ort. Die Datei wird `.bwl` als Erweiterung haben.

Um eine zuvor gespeicherte Freundesliste zu laden, klicken Sie **Laden** und öffnen die entsprechende `.bwl` Datei. Um den Inhalt einer aktuellen Liste zurückzusetzen während der Inhalt einer zuvor gespeicherten Liste geladen wird, wählen Sie **Liste beim Laden leeren**.



Anmerkung

Wir empfehlen, dass Sie die Namen Ihrer Freunde und deren E-Mail-Adressen der **Freundesliste** hinzufügen, damit sichergestellt ist, dass nur solche E-Mails an Sie weitergeleitet werden.

Klicken Sie auf **Übernehmen** und **OK**, um zu speichern und um die **Freundesliste** zu schließen.

- **Einstellungen** - Öffnet das Fenster **Einstellungen**, indem Sie weitere Optionen für das **Antispam**-Modul angeben können.



Einstellungen

Die folgenden Optionen sind verfügbar:

- **Nachrichten nach "Gelöschte Objekte" verschieben** verschiebt als Spam erkannte E-Mails in einen Unterordner des **Papierkorbs** (gilt nur für Outlook Express bzw. Windows Mail).
- **Nachricht als gelesen markieren** - markiert alle Spam Nachrichten als gelesen und stört somit den Arbeitsablauf nicht, wenn neue Nachrichten eintreffen.

Wenn Ihr Antispam-Filter ungenau arbeitet, sollten Sie die Filter-Datenbank löschen und den Bayesian-Filter neu trainieren. Klicken Sie auf **Antispam Datenbank leeren**, um danach die Bayesian Datenbank neu aufzubauen.

Sie können die Bayesianische Datenbank in eine Datei speichern um Sie für andereAcronis Internet Security Suite 2010 Produkte oder nach einer Neuinstallation zu verwenden. Um die Trainingsdatenbank des bayesischen Filters zu speichern klicken Sie den Button **Bayes speichern** und wählen Sie den gewünschten Speicherort. Die Datei wird `.dat` als Erweiterung haben.

Um eine gsicherte Bayesianische Datenbank zu laden, wählen Sie **Loade Bayes** und öffnen die entsprechende Datei.

Klicken Sie auf **Alarma**, um Zugriff auf die Sektion haben, in der Sie die Erscheinung des Bestätigungsfensters für **Spammer hinzufügen** und **Freunde hinzufügen** deaktivieren können.



Anmerkung
In dem **Alarma** Fenster können Sie den Alarm **Bitte wählen Sie eine E-Mail-Nachricht** aktivieren/deaktivieren.Dieses Alarm erscheint wenn Sie eine Gruppe anstatt einer E-Mail-Nachricht auswählen.

- **Assistent** - öffnet den Antispam Konfigurationsassistenten, welcher beim trainieren des Bayesianischen Filters hilft, um die Effizienz des Acronis Internet Security Suite 2010 Antispam-Filters weiter zu steigern. Sie können auch Adressen auch aus Ihrem Adreesbuch zum Freunde-/Spammer Liste hinzufügen.
- **Acronis Internet Security Suite Antispam** - öffnet die Acronis Internet Security Suite 2010 Benutzeroberfläche.

Wie man

31. Wie man Datein und Ordner prüft

Prüfen mit Acronis Internet Security Suite 2010 ist einfach und flexibel. Es gibt 4 Arten um Acronis Dateien und Ordner auf Viren und andere Maleware prüfen zu lassen:

- Unter Verwendung des Windows Kontext Menus
- Unter Verwendung von Prüfaufgaben
- Unter Verwendung der Acronis manuellen Prüfung
- Unter Verwendung der Aktivitätsanzeige

Sobald Sie die Prüfung eingeleitet haben wird der Antivirus Prüfassistent erscheinen und Sie durch den Handlungsprozess leiten. Weitere Informationen zu diesem Assistenten finden Sie unter *„Antivirus Prüfassistent“* (S. 44).

31.1. Unter Verwendung des Windows Kontext Menus

Dies ist der einfachste und empfohlene Weg eine Datei oder Ordner auf Ihrem Computer zu prüfen. Rechtsklicken Sie das zu prüfende Objekt und wählen Sie **Scanne mit Acronis Internet Security Suite** aus dem Menü aus. Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen.

Typische Situationen in welchen Sie diese Prüfmethode verwenden würden schliessen das Folgende ein:

- Sie verdächtigen eine bestimmte Datei oder Ordner infiziert zu sein.
- Wann immer Sie vom Internet Dateien herunterladen von denen Sie glauben infiziert zu sein.
- Prüfen Sie einen freigegebnen Ordner bevor Sie von ihm Dateien auf Ihren Rechner kopieren.

31.2. Unter Verwendung von Prüfaufgaben

Wenn Sie Ihren Computer oder bestimmte Ordner regelmässig prüfen lassen möchten, so sollten Sie in Betracht ziehen hierfür eine Prüfaufgabe zu verwenden. Prüfaufgaben weisen Acronis Internet Security Suite 2010 an wo zu prüfen und welche Option und Aktion zu tätigen ist. Ausserdem, können Sie planen sie auf geregelter Basis oder zu einer bestimmten Zeit laufen zu lassen.

Um Ihren Computer unter Verwendung von Prüfaufgaben prüfen zu lassen, öffnen Sie die Acronis Internet Security Suite 2010 Benutzeroberfläche und starten dort die gewünschte Prüfaufgabe. Abhängig von der Benutzeransicht, ist verschiedenen Schritten zur Durchführung einer Prüfaufgabe zu folgen.

Starten von Prüfaufgaben in der Basisansicht

In der Basisansicht, kann nur eine Standardprüfung des gesamten PC's gestartet werden, klicken Sie **Jetzt prüfen**. Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen.

Starten von Prüfaufgaben in der Mittleren Ansicht

In der Mittleren Ansicht können Sie eine Reihe von vorkonfigurierten Prüfaufgaben starten. Zudem können benutzerdefinierte Prüfaufgaben konfiguriert und gestartet werden um bestimmte Bereiche Ihres PC's zu prüfen. Folgen Sie diesen Schritten um eine Prüfaufgabe in der Mittleren Ansicht zu starten:

1. Klicken Sie das **Security** Tab.
2. Auf der linken Seite, im Quick Task-Bereich, klicken Sie **Systemprüfung** um eine Standardprüfung des gesamten PC'c zu starten. Um eine andere Prüfung zu starten, klicken Sie den Pfeil auf der Schaltfläche und wählen die gewünschte Aufgabe. Um eine benutzerdefinierte Prüfung zu konfigurieren und zu starten, klicken Sie **benutzerdefinierte Prüfung**. Dieses sind die verfügbaren Prüfaufgaben:

Prüfaufgabe	Beschreibung
Systemprüfung	Prüft alle Dateien mit Ausnahme von Archiven. In der standard Konfiguration, wird nach allen Arten von Malware geprüft, ausser rootkits.
Tiefgehende Systemprüfung	Prüft das komplette System In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Meine Dokumente prüfen	Verwenden Sie diese um die folgenden für den jeweiligen Benutzer wichtigen Ordner zu prüfen: `Eigene Dateien`, `Desktop` und `Autostart`. Dies stellt sicher das Ihre Eigenen Dateien, Ihr Desktop und die beim Starten von Windows geladenen Programme schädlingsfrei sind.
Prüfung anpassen	Diese Option erlaubt es Ihnen angepasste Prüfvorgänge zu erstellen und auszuführen. Sie können festlegen was geprüft werden soll und weitere Prüfparameter festlegen. Sie können angepasste Prüfvorgänge speichern und auf diese später im fortgeschrittenen oder im Profi-Modus wieder zugreifen.

3. Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen. Falls Sie eine benutzerdefinierte Prüfung durchführen, muss zuvor der entsprechende Assistent abgeschlossen werden.

Starten von Prüfaufgaben in der Profiansicht

In der Profiansicht können Sie alle vorkonfigurierten Prüfaufgaben durchführen und deren Prüfoptionen ändern. Ausserdem können Sie dort Prüfaufgaben selbst erstellen wenn Sie an bestimmten Stellen Ihres Computers prüfen möchten. Folgen Sie den Schritten um eine Prüfaufgabe in der Profiansicht zu starten:

1. Klicken Sie auf **Antivirus** in dem Menü auf der linken Seite.
2. Klicken Sie auf den Tab **Virenscan** Hier finden Sie eine Reihe von Standartprüfaufgaben und Sie können hier Ihre eigenen Prüfaufgaben erstellen. Dies sind die Standartprüfaufgeben welche Sie verwenden können:

Standard Einstellungen	Beschreibung
Tiefgehende Systemprüfung	Prüft das komplette System In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Systemprüfung	Prüft alle Dateien mit Ausnahme von Archiven. In der standard Konfiguration, wird nach allen Arten von Malware geprüft, ausser rootkits.
Schnelle Systemprüfung	Prüft dieWindows und Programme Ordner. In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, ausgenommen Rootkits. Ausserdem wird der Arbeitspeicher, die Registy und Cookies nicht geprüft.
Meine Dokumente	Verwenden Sie diese um die folgenden für den jeweiligen Benutzer wichtigen Ordner zu prüfen: Eigene Dateien, Desktop und Autostart. Dies stellt sicher das Ihre Eigenen Dateien, Ihr Desktop und die beim Starten von Windows geladenen Programme schädlingsfrei sind.

3. Doppelklicken Sie die Prüfaufgabe die Sie zu starten wünschen.
4. Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen.

31.3. Unter Verwendung der Acronis manuellen Prüfung

Acronis manuelle Prüfung lässt sie eine Prüfung eines bestimmten Ordners oder einer Festplattenpartition durchführen ohne das Erstellen einer Prüfaufgabe. Diese

Funktion wurde implimentiert zur Verwendung im abgesicherten Modus von Windows. Falls Ihr System mit einem anpassungfähigen Virus infiziert wurde, so können Sie versuchen diesen zu entfernen indem Sie Windows im abgesicherten Modus starten und mit der manuellen Prüfung von Acronis jede Festplattenpartition scannen.

Um Ihren Computer unter Verwendung der manuellen Prüfung zu prüfen, folgen Sie den Schritten:

1. Im start Windows Start Menu, folgen Sie dem Pfad**Start → Programme → Acronis Internet Security Suite 2010 → Acronis manuelle Prüfung**. Ein neues Fenster wird sich öffnen.
2. Klicken Sie auf **Hinzufügen**, um das Prüfziel auszuwählen. Ein neues Fenster wird sich öffnen.
3. Wählen Sie das Prüfziel:
   - Um Ihr Desktop zu prüfen, wählen sie einfach **Desktop**.
   - Um eine komplette Festplattenpartition prüfen zu lassen, wählen Sie sie unter Arbeitsplatz aus.
   - Um einen bestimmten Ordner zu prüfen, suchen Sie ihn heraus und wählen ihn aus.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Weiter** um die Prüfung zu starten.
6. Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen.

Was ist Abgesichertes Modus?
Der abgesicherte Modus ist eine Sonderfunktion von Windows, welche in den meisten Fällen zur Behebung von Problemen, die normale Operationen von Windows beeinflussen, verwendet wird. Solche Probleme reichen von Treiberkonflikten, bis hin zu Viren welche Windows am normalen Starten hindern. Im abgesicherten Modus lädt Windows nur die nötigsten Betriebssystemkomponenten und Basistreiber. Nur wenige Anwendungen funktionieren im abgesicherten Modus. Das ist der Grund warum die meisten Viren im abgesicherten Modus inaktiv und somit einfach zu entfernen sind.
Um Windows im abgesicherten Modus zu starten, starten Sie ihren Rechner neu und drücken die F8 Taste bis das Windows Erweiterte Optionen Menu erscheint. Sie können zwischen mehreren Optionen wählen. Sie können **abgesicherter Modus mit Netwerktreibern wählen** um auch Internetzugriff zu haben.



Anmerkung

Um mehrere Informationen über Abgesichertes Modus herauszufinden, öffnen Sie die Windows Hilfe/Support (Klicken Sie im Startmenu auf **Hilfe und Support**). Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.

31.4. Aktivitätsanzeige

Die **Scan Aktions-Anzeige** ist eine graphische Visualisierung der Prüfaktivität auf Ihrem System. Dieses kleine Fenster ist standardmässig nur verfügbar in der Profi-Ansicht.



Scanaktivitsänzeige

Sie können die Aktivitätsanzeige verwenden um kurzerhand Dateien und Ordner zu prüfen. Ziehen Sie & die gewünschte Datei oder Ordner um sie zu prüfen in die Aktivitätsanzeige. Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen.



Anmerkung

Für weitere Informationen lesen Sie bitte„*Scanaktivitsänzeige*“ (S. 27).

32. Wie man eine Systemprüfung einplant

Ihren Computer regelmässig prüfen zu lassen ist die beste Art ihn frei von Maleware zu halten. Acronis Internet Security Suite 2010 gibt Ihnen die Möglichkeit Prüfaufgaben einzuplanen so das Sie Ihren Computer automatisch prüfen lassen können.

Um Acronis Internet Security Suite 2010 eine geplante Prüfaufgabe durchführen zu lassen folgen Sie den Schritten:

1. Öffnen Sie Acronis Internet Security Suite 2010 und wechseln Sie in die Profi-Ansicht.
2. Klicken Sie auf **Antivirus** in dem Menü auf der linken Seite.
3. Klicken Sie auf den Tab **Virenscan** Hier finden Sie eine Reihe von Standartprüfaufgaben und Sie können hier Ihre eigenen Prüfaufgaben erstellen.
   - Systemaufgaben sind verfügbar und können unter jedem Windows Benutzerkonto gestartet werden.
   - Benutzeraufgaben sind ausschliesslich für den Benutzer verfügbar der sie erstellt hat und können auch nur von diesem gestartet werden.

   Dies sind die Standartprüfaufgeben welche Sie einplanen können:

Standard Einstellungen	Beschreibung
Tiefgehende Systemprüfung	Prüft das komplette System In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Systemprüfung	Prüft alle Dateien mit Ausnahme von Archiven. In der standard Konfiguration, wird nach allen Arten von Malware geprüft, ausser rootkits.
Schnelle Systemprüfung	Prüft die`Windows` und `Programme` Ordner. In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, ausgenommen Rootkits. Ausserdem wird der Arbeitspeicher, die Registy und Cookies nicht geprüft.
Prüfung bei Login	Prüft die Objekte, die ausgeführt werden, wenn ein Benutzer sich bei Windows anmeldet. Um diese Aufgabe zu nutzen, muss sie eingeplant werden beim Systemstart zu laufen. Standardmäßig ist die Prüfung im Hintergrund deaktiviert.
Meine Dokumente	Verwenden Sie diese um die folgenden für den jeweiligen Benutzer wichtigen Ordner zu prüfen:

Standard Einstellungen	Beschreibung
	`Eigene Dateien`, `Desktop` und `Autostart`. Dies stellt sicher das Ihre Eigenen Dateien, Ihr Desktop und die beim Starten von Windows geladenen Programme schädlingsfrei sind.

Falls keine der Prüfaufgaben Ihren Bedürfnissen entspricht können Sie eine neue Prüfaufgabe erstellen, welche Sie dann wiederum so einplanen können wie Sie wünschen.

4. Rechtsklicken Sie die gewünschte Prüfaufgabe und wählen Sie **Eingeplant**. Ein neues Fenster wird sich öffnen.
5. Planen Sie die Aufgabe ein wie erforderlich:
   - Um die Aufgabe einmalig durchzuführen, wählen Sie **Einmalig** und bestimmen Sie das Startdatum und die Zeit.
   - Um die Prüfaufgabe nach dem Systemstart, wählen Sie **Beim Systemstart**. Geben Sie an wie lange nach dem Systemstart die Aufgabe gestartet sein wird.(Minuten)
   - Um die Aufgabe auf regulärer Basis laufen zu lassen, wählen Sie **Periodisch** und bestimmen Sie die Häufigkeit, das Startdatum und die Zeit.



Anmerkung

Als Beispiel, um Ihren Computer jeden Samstag um 2:00Uhr prüfen zu lassen, müssen Sie wie folgt einplanen:

a. Wählen Sie **Periodisch**.

b. Im **Täglich** Feld, geben Sie 1 ein und wählen dann**Wochen** im Menu. Auf diese Art wird die Aufgabe einmal wöchentlich laufen.

c. Legen Sie als Startdatum den kommenden Samstag fest.

d. Legen Sie als Startzeit `2:00:00 Uhr`fest.

6. Klicken Sie **OK** um die Planung zu speichern. Die Prüfaufgabe wird automatisch, gemäß der definierten Planung, ablaufen. Falls der Computer im Moment der geplanten Aufgabe abgeschaltet ist, so wird die Aufgabe beim nächsten Computerstart starten.

Fehlediagnose und Problemlösung

33. Problemlösung

Dieses Kapitel zeigt einige Probleme bei der Benutzung von Acronis Internet Security Suite 2010 auf und bietet mögliche Lösungen dazu. Die meisten dieser Probleme können durch die geeigneten Einstellungen im Produkt behoben werden.

Wenn Sie Ihr Problem hier nicht finden oder dieser weiterhin besteht, können Sie kontakt zu unserem Acronis Technischen Support aufnehmen, wie beschrieben in *„Support“* (S. 318).

33.1. Installationsprobleme

Dieser Artikel hilft Ihnen, die allgemeinsten Installationsprobleme mit Acronis Internet Security Suite 2010 zu überprüfen. Diese Probleme können in die folgenden Kategorien gruppiert werden:

- Installationsgültigkeitsstörungen: der Einstellungsassistent kann wegen spezifische Bedingungen auf Ihrem System nicht laufen.
- Installation fehlgeschlagen: Sie haben eine Installation vom Einstellungsassistenten gestartet, wurde aber nicht erfolgreich abgeschlossen.

33.1.1. Installationsgültigkeitsstörungen

Beim Start des Einstellungsassistenten ist eine Anzahl von Bedingungen zu erfüllen um zu gewährleisten dass die Installation starten kann. Die folgende Tabelle zeigt Ihnen die häufigsten Problemquellen während der Installation und mögliche Methoden um diese zu beheben.

Fehler	Beschreibung&Lösung
Sie haben nicht genügende Rechte um das Programm zu installieren.	Um den Einstellungsassistent zu starten und Acronis Internet Security Suite 2010 zu installieren, benötigen Sie Administratorrechte. Wählen Sie eine der folgenden Methoden: ● Melden Sie sich am Windows mit einen Administratorkonto ein und starten Sie den Einstellungsassistent erneut. ● Klicken Sie mit der rechten Maustaste auf die Installationsdatei und wählen Sie **Ausführen als...**. Geben Sie den Benutzername und Passwort des Windows Administratorskonto ein.
Der Installer hat eine frühere Version von Acronis	Acronis Internet Security Suite 2010 war vorher auf Ihr System installiert, aber die Installation wurde nicht

Fehler	Beschreibung&Lösung
Internet Security Suite 2010 erkannt, die nicht korrekt deinstalliert wurde.	vollständig entfernt. Diese blockiert eine neue Installation von Acronis Internet Security Suite 2010. Um diese Problem zu überwinden und Acronis Internet Security Suite 2010 zu installieren, folgen Sie diesen Schritten: 1. Kontaktieren Sie, wie unter *„Support“* (S. 318) beschrieben, den technischen Support von Acronis und fragen Sie nach dem Deinstallations-Tool. 2. Starten Sie das Uninstall Tool durch benutzung der Adminstratorrechte. 3. Bitte starten Sie Ihren Computer neu. 4. Starten Sie den Installationsassistenten erneut um Acronis Internet Security Suite 2010 zu installieren.
Das Acronis Internet Security Suite 2010-Produkt ist mit Ihrem Betriebssystem nicht kompatibel.	Sie versuchen Acronis Internet Security Suite 2010 auf einen nicht unterstützten Betriebsystem zu installieren. Besuchen Sie bitte *„Systemanforderungen“* (S. 2) um herauszufinden auf was für einen Betriebsystem Sie Acronis Internet Security Suite 2010 installieren können. Ihr Betriebssystem ist Windows XP mit Service Pack 1 oder niedriger, Sie können Service Pack 2 oder einen höheren installieren und den Einrichtungsassistent erneut ausführen.
Die Installationsdatei wurde für eine andere Art von Prozessoren entwickelt.	Wenn Sie eine solche Fehlermeldung erhalten, dann bedeutet das, dass Sie eine falsche Version der Installationsdatei ausführen. Es gibt Zwei Versionen der Acronis Internet Security Suite 2010 Installationsdatei: eine für 32-bit Prozessoren und eine andere für 64-bit Prozessoren. Um sicher zu gehen dass Sie die richtige Version für Ihren System erhalten, laden Sie die Installationsdatei bitte von hier herunter:http://www.acronis.de.

33.1.2. Installation fehlgeschlagen

Es gibt mehrere Installationsausfallmöglichkeiten:

- Während der Installation, erscheint ein Störungsfenster. Sie erhalten möglicherweise eine Nachricht zum Abbrechen der Installation oder um das "Uninstall Tool" zu starten um Reste einer früheren Installation zu entfernen.



Anmerkung

Nach dem Start der Installation erhalten Sie möglicherweise eine Benachrichtigung, daß nicht genügend freier Speicherplatz auf Ihrer Festplatte zur Verfügung steht. In diesem Fall müssen Sie den benötigten Platz auf der Zielpartition frei machen und danach die Installation fortsetzen oder neu starten.

- Die Installation hängt und möglicherweise friert Ihr System ein. Nur einen Neustart stellt den Systemsreaktionsvermögen wieder her.
- Installation wurde abgeschlossen, aber Sie können einige oder alle Acronis Internet Security Suite 2010 Funktionen nicht verwenden.

Um eine Fehl-Installation zu überprüfen und Acronis Internet Security Suite 2010 zu installieren, folgen Sie diesen Schritten:

1. **Reinigen Sie das System nach der Fehlinstallation.** Falls die Installation fehlschlägt, bleiben einige Acronis Internet Security Suite 2010 Registry-Schlüssel und Dateien in Ihrem System. Solche Rückstände können eine erneute Installation verhindern. Ebenso kann die Systemleistung und Stabilität leiden. Aus diesem Grund müssen diese vor einer erneuten Produktinstallation entfernt werden.

   Wenn die Fehlermeldung einen Knopf anzeigt, um ein Uninstall Tooll auszuführen, klicken Sie diesen an, um das System zu reinigen. Andernfalls gehen Sie folgendermaßen vor:

   a. Kontaktieren Sie, wie unter „*Support*“ (S. 318) beschrieben, den technischen Support von Acronis und fragen Sie nach dem Deinstallations-Tool.

   b. Starten Sie das Uninstall Tool durch benutzung der Adminstratorrechte.

   c. Bitte starten Sie Ihren Computer neu.

2. Überprüfen Sie, ob Sie irgendeine andere Sicherheitslösung installiert haben, weil diese den Normalbetrieb von Acronis Internet Security Suite 2010 stören könnte. Wenn dies der Fall ist, empfehlen wir Ihnen alle anderen Sicherheitslösungen zu entfernen und Acronis Internet Security Suite 2010 wieder neu zu installieren.
3. Versuchen Sie erneut Acronis Internet Security Suite 2010 zu installieren. Es wird empfohlen dass Sie die aktuellste Version der Installationsdatei von www.acronis.de herunterladen und ausführen.
4. Wenn die Installation wieder fehlschlägt, nehmen Sie bitte kontakt zum Acronis Inc. Support auf, wie beschrieben in „*Support*“ (S. 318).

33.2. Acronis Internet Security Suite 2010 Dienste antworten nicht

Dieser Artikel hilft Ihnen bei der Lösung des *Acronis Internet Security Suite 2010 Dienste antworten nicht* Problems. Diese Fehlermeldung kann folgendermassen auftauchen:

- Das Acronis Symbol in System Tray ist ausgegraut und ein Pop-up informiert Sie, dass die Acronis Internet Security Suite 2010 Dienste nicht Antworten.
- Das Acronis Internet Security Suite 2010 Fenster zeigt an, dass die Acronis Internet Security Suite 2010 Dienste nicht Antworten.

Der Fehler kann durch einen der folgenden Bedingungen verursacht werden:

- ein wichtiges Update wird installiert.
- temporäre Kommunikationsstörungen zwischen den Acronis Internet Security Suite 2010 Dienste.
- einige der Acronis Internet Security Suite 2010 Dienste sind gestoppt.
- andere Sicherheitslösungen laufen gleichzeitig wie Acronis Internet Security Suite 2010 auf Ihren Rechner.
- Viren auf Ihrem System beeinflussen den Normalbetrieb von Acronis Internet Security Suite 2010.

Um diese Störung zu überprüfen, versuchen Sie diese Lösungen:

1. Warten Sie einen Moment und sehen Sie ob sich was ändert. Die Störung könnte temporär sein.
2. Starten Sie den Rechner neu und warten Sie einige Momente, bis Acronis Internet Security Suite 2010 geladen ist. Öffnen Sie Acronis Internet Security Suite 2010 und überprüfen Sie ob das Problem immernoch besteht. Das neustarten des Rechners behebt normalerweise das Problem.
3. Überprüfen Sie, ob Sie irgendeine andere Sicherheitslösung installiert haben, weil diese den Normalbetrieb von Acronis Internet Security Suite 2010 stören könnte. Wenn dies der Fall ist, empfehlen wir Ihnen alle anderen Sicherheitslösungen zu entfernen und Acronis Internet Security Suite 2010 wieder neu zu installieren.
4. Wenn das Problem weiterhin besteht, kann es sich um ein ernsteres Problem handeln (z.B., können der Rechner mit einem Virus infiziert sein, wodurch Acronis Internet Security Suite 2010 behindert wird). Bitte kontaktieren Sie den Acronis Inc. Support wie im Abschnitt *„Support“* (S. 318) beschrieben.

33.3. Datei und Druckerfreigabe im Wi-Fi (Drathlos) Netzwerk funktioniert nicht.

Dieser Artikel hilft Ihnen, die folgenden Probleme mit der Acronis Internet Security Suite 2010 Firewall in den Wi-Fi Netzwerken zu lösen:

- Dateifreigabe mit Rechnern die sich in einem Wi-Fi Netzwek befinden, nicht möglich.
- Kein Zugriff auf einen Netzwerkdrucker der sich in einem Wi-Fi Netzwerk befindet.
- Kein Zugriff auf einen Netzwerkdrucker, freigegeben durch einen anderen Rechner, der sich in einem Wi-Fi Netzwerk befindet.
- Eigene Druckerfreigabe mit anderen Rechner in Wi-Fi Netzwerk funktioniert nicht.

Bevor Sie anfangen, diese Probleme zu überprüfen, sollten Sie einige Sachen über die Sicherheit und die Acronis Internet Security Suite 2010 Firewallkonfiguration in Wi-Fi Netzwerken wissen. Von einem Sicherheit Standpunkt, gehören Wi-Fi Netzwerke zu einem der folgenden Kategorien:

- **Gesicherte Wi-Fi Netzwerke.** Diese Art von Netzwerk erlaubt nur berechtigte Wi-Fi-aktive Geräte sich zu verbinden. Für den Netzzugang wird ein Kennwort benötigt. Beispiele der gesicherten Wi-Fi Netzwerke sind diese, die in den Büronetzwerken gegründet wurden.
- **Offene (Ungesicherte) Wi-Fi Netzwerken.** Man kann Problemlos auf jeden Wi-FI-aktives Gerät innerhalb des Bereiches eines ungesicherten Wi-Fi Netzwerks verbunden werden. Ungesicherte WLAN Netzwerke sind weit verbreitet. Dies betrifft z.B. öffentliche WLAN Hotspots in Schulen, Restaurants, Flughäfen usw. Ein Heimnetzwerk mit einem WLAN Router ist ebenfalls ungesichert bis entsprechende Sicherheits-Einstellungen am Router getätigt wurden.

  Ungesicherte Wi-Fi Netzwerke stellen ein großes Sicherheitsrisiko dar, da Ihr Computer an unbekannte Computer angeschlossen ist. Ohne einen korrekten Schutz, der von einer Firewall geboten wird, kann jeder, der an das Netz angeschlossen ist, auf Ihre Freigaben zugreifen und in Ihren Computer sogar einbrechen.

Wenn Sie mit einen ungesichertes Wi-Fi Netzwerk verbunden sind, wird Acronis Internet Security Suite 2010 alle Verbindungen mit diesen Netzwerk automatisch blockieren. Sie werden nue auf das Internet zugriff haben, können aber keine Dateien oder Drucker freigeben.

Es bestehen zwei Möglichkeiten um die Kommunikation mit einem Wi-Fi Netzwerk zu ermöglichen:

- Der "Vertrauenswürdige Computer"Lösung erlaubt Datei und Druckerfreigabe, nur mit spezifische Computer (Vertrauenswürdige Computer) im Wi-Fi Netzwerks. Verwenden Sie diese Lösung wenn Sie mit einem öffentlichen Wi-Fi Netzwerk

verbunden sind (z.B.: Kampus oder im Cafe) und Sie Dateien oder Drucker mit jemandem teilen.

- Die "Sicheres Netzwerk" Lösung Datei und Druckerfreigabe für das gesamte Wi-Fi Netzwerk. Diese Lösung wird aus Sicherheitsgründe nicht empfohlen, kann aber in besondere Situationen nützlich sein (z.B., können Sie es für ein Heim- oder Büro Wi-Fi -Netzwerk verwenden).

33.3.1. "Vertrauenswürdige Computer"-Lösung

Um die Acronis Internet Security Suite 2010 Firewall so zu konfigurieren, daß Sie Dateien oder Drucker im WLAN Netzwerk anbieten oder selbst auf Netz-Drucker zugreifen können, befolgen Sie folgende Schritte:

1. Öffnen Sie Acronis Internet Security Suite 2010 und wechseln Sie in die Profi-Ansicht.
2. Klicken Sie auf **Firewall** im Menü auf der linken Seite.
3. Klicken Sie auf den Tab **Netzwerk**.
4. In der Tabelle mit Zonen, wählen Sie Wi-Fi Netzwerk und klicken Sie auf **Hinzufügen**.
5. Wählen Sie den gewünschten Computer- oder Wi-Fi Netzwerkdrucker von der Liste der Geräte, die im Wi-Fi Netzwerk entdeckt wurden. Wenn dieser Computer oder Drucker nicht automatisch entdeckt wurde, können Sie dessen IPaddresse im **Zonen** Feld eintragen.
6. Wählen Sie **Erlauben**.
7. Klicken Sie auf **OK**.

Wenn Sie Datein oder einen Drucker nicht mit dem vorgewählten Computer freigeben können, wird dieses höchstwahrscheinlich nicht durch die Acronis Internet Security Suite 2010 Firewall auf Ihrem Computer verursacht. Überprüfen Sie andere mögliche Ursachen, wie z.B:

- Die Firewall auf dem anderen Computer kann Dateien und Druckerfreigabe die sich in einen ungesicherten Wi-fi Netzwerk befinded, blockieren.
  - ▶ Wenn die Acronis Internet Security Suite 2010 Firewall verwendet wird, muss dieselbe Prozedur auf allen anderen Computer nachvollzogen werden, um eine Datei- und Druckerfreigabe mit Ihrem Computer zu ermöglichen.
  - ▶ Wenn die Windows Firewall benutzt wird, kann diese so konfiguriert werden um Datei und Druckerfreigabe, wie gefolgt, zu erlauben: öffnen Sie die Windows Firewall Einstellungsfenster, unter **Ausnahme** wählen Sie die option **Datei- und Druckerfreigabe**.
  - ▶ Wenn eine andere Firewall verwendet wird, beziehen Sie sich bitte auf dessen Unterlagen oder Hilfsdateien.

- Allgemeine Bedingungen, die die Benutzung oder Verbindung an den freigegebenen Drucker verhindern können:
  - Möglicherweise müssen Sie sich mit einen Windows Adminstratorkonto anmelden um auf die Druckerfreigabe zugreifen zu können.
  - Rechte werden für den freigegebenen Drucker gesetzt so dass dieser nur spezifische Computer und Benutzer erlaubt. Falls Sie Ihren Drucker freigegeben haben, überprüfen Sie die Rechte, die für den Drucker gesätzt sind, um zu sehen, ob der Benutzer auf dem anderen Computer, der Zugang zum Drucker erlaubt wird. Wenn Sie versuchen eine Verbindung zum freigegebenen Drucker aufzubauen, sollten Sie mit Benutzer auf dem anderen Computer überprüfen, ob Sie die benötigte Rechte haben.
  - Der Drucker der mit Ihren Computer oder einem anderen verbunden ist, ist nicht freigegeben.
  - Der freigegebene Drucker wurde an dem Computer nicht hinzugefügt.



Anmerkung
Um mehr darüber zu erfahren, wie Sie die Druckerfreigabe verwalten können um Drucker im Netz freizugeben oder die Rechte anzupassen, öffnen sie im Windows-Startmenü **Hilfe und Support**).

Wenn keine verbindung zu Wi-Fi Netzwerkdrucker besteht, wird dieses höchstwahrscheinlich nicht durch die Acronis Internet Security Suite 2010 Firewall auf Ihrem Computer verursacht Der Zugriff auf Netzwerk-Drucker über das WLAN könnte auf bestimmte Computer oder Nutzer beschränkt sein. Fragen Sie Ihren Netzwerk-Administrator, ob Sie die notwendigen Rechte besitzen um auf diesen Drucker zuzugreifen.

Wenn Sie vermuten das dieser Problem in Zusammenhang mit der Acronis Internet Security Suite 2010 Firewall besteht, können Sie wie hier beschrieben, den Acronis Support kontaktieren: *„Support“* (S. 318).

33.3.2. "Sicheres Netzwerk" Lösung

Es wird empfohlen diese Lösung nur für Heim und Büro Wi-Fi Netzwerke zu benutzen.

Um Acronis Internet Security Suite 2010 Firewall so zu konfigurieren das dieser alle Dateien und Druckerfreigaben in einem Wi-Fi Netzwerk erlaubt, follgen Sie diese Schritte:

1. Öffnen Sie Acronis Internet Security Suite 2010 und wechseln Sie in die Profi-Ansicht.
2. Klicken Sie auf **Firewall** im Menü auf der linken Seite.
3. Klicken Sie auf den Tab **Netzwerk**.

4. In der Netzwerk-Konfigurations-Tabelle, Spalte **Vertrauensstufe**, klicken Sie den zum WLAN Netzwerk gehörenden Pfeil ▾.
5. Abhängig von der Sicherheitsstufe, die Sie erreichen möchten, wählen Sie eine der folgenden Optionen:
   - **Unsicher** um auf die Datein und Druckerfreigaben in Wi-Fi Netzwerk zuzugreifen, ohne den Zugrif auf Ihre freigaben zu erlauben.
   - **Sicher** um Datei und Druckerfreigabe auf beide Seiten zu erlauben. Das bedeutet dass der Benutzer der am Wi-Fi Netzwerk verbunden ist, kann auch Ihre freigegebenen Daten und Drucker zugreifen.

Wenn Sie Datein oder einen Drucker nicht mit dem vorgewählten Computer freigeben können, wird dieses höchstwahrscheinlich nicht durch die Acronis Internet Security Suite 2010 Firewall auf Ihrem Computer verursacht. Überprüfen Sie andere mögliche Ursachen, wie z.B:

- Die Firewall auf dem anderen Computer kann Dateien und Druckerfreigabe die sich in einen ungesicherten Wi-fi Netzwerk befinded, blockieren.
  - ▶ Wenn die Acronis Internet Security Suite 2010 Firewall verwendet wird, muss dieselbe Prozedur auf allen anderen Computer nachvollzogen werden, um eine Datei- und Druckerfreigabe mit Ihrem Computer zu ermöglichen.
  - ▶ Wenn die Windows Firewall benutzt wird, kann diese so konfiguriert werden um Datei und Druckerfreigabe, wie gefolgt, zu erlauben: öffnen Sie die Windows Firewall Einstellungsfenster, unter **Ausnahme** wählen Sie die option **Datei- und Druckerfreigabe**.
  - ▶ Wenn eine andere Firewall verwendet wird, beziehen Sie sich bitte auf dessen Unterlagen oder Hilfsdateien.
- Allgemeine Bedingungen, die die Benutzung oder Verbindung an den freigegebenen Drucker verhindern können:
  - ▶ Möglicherweise müssen Sie sich mit einen Windows Adminstratorkonto anmelden um auf die Druckerfreigabe zugreifen zu können.
  - ▶ Rechte werden für den freigegebenen Drucker gesetzt so dass dieser nur spezifische Computer und Benutzer erlaubt. Falls Sie Ihren Drucker freigegeben haben, überprüfen Sie die Rechte, die für den Drucker gesätzt sind, um zu sehen, ob der Benutzer auf dem anderen Computer, der Zugang zum Drucker erlaubt wird. Wenn Sie versuchen eine Verbindung zum freigegebenen Drucker aufzubauen, sollten Sie mit Benutzer auf dem anderen Computer überprüfen, ob Sie die benötigte Rechte haben.
  - ▶ Der Drucker der mit Ihren Computer oder einem anderen verbunden ist, ist nicht freigegeben.
  - ▶ Der freigegebene Drucker wurde an dem Computer nicht hinzugefügt.



Anmerkung

Um mehr darüber zu erfahren, wie Sie die Druckerfreigabe verwalten können um Drucker im Netz freizugeben oder die Rechte anzupassen, öffnen sie im Windows-Startmenü **Hilfe und Support**).

Wenn keine verbindung zu Wi-Fi Netzwerkdrucker besteht, wird dieses höchstwahrscheinlich nicht durch die Acronis Internet Security Suite 2010 Firewall auf Ihrem Computer verursacht Der Zugriff auf Netzwerk-Drucker über das WLAN könnte auf bestimmte Computer oder Nutzer beschränkt sein. Fragen Sie Ihren Netzwerk-Administrator, ob Sie die notwendigen Rechte besitzen um auf diesen Drucker zuzugreifen.

Wenn Sie vermuten das dieser Problem in Zusammenhang mit der Acronis Internet Security Suite 2010 Firewall besteht, können Sie wie hier beschrieben, den Acronis Support kontaktieren: *„Support“* (S. 318).

33.4. Antispamfilter funkioniert nicht richtig

Dieser Artikel hilft Ihnen, die folgenden Probleme mit der Acronis Internet Security Suite 2010 Antispamfilter lösen:

- Eine Anzahl von seriösen E-Mails werden markiert als `[spam]`.
- Viele Spams werden entsprechend nicht durch den Antispam Filter markiert.
- Der Antispam-Filter entdeckt keine Spamnachrichten.

33.4.1. Seriöse Nachrichten werden markiert als [spam]

Seriöse Nachrichten werden markiert als `[spam]` schlicht weil sie für den Acronis Internet Security Suite 2010 Antispam Filter wie solche aussehen. Im Normalfall können Sie dieses Problem lösen indem Sie den Antispam Filter angemessen konfigurieren.

Acronis Internet Security Suite 2010 fügt die Empfänger Ihrer Mails automatisch der Freundesliste hinzu. Die erhaltenen E-Mail der in der Freundesliste geführten Kontakte werden als seriös angesehen. Sie werden nicht vom Antispam Filter geprüft und deshalb auch nicht als `[spam]` markiert.

Die automatische Konfiguration der Freundesliste verhindert nicht die entdeckte Störungen, die in dieser Situationen auftreten können:

- Sie empfangen viele angeforderte Werb-E-Mails resultierend aus der Anmeldung auf verschiedene Webseiten. In diesem Fall ist die Lösung, die E-Mail Adressen, von denen Sie solche E-Mails bekommen, auf die Freunde Liste zu setzen.
- Ein erheblicher Teil Ihrer legitimen Email ist von Leuten, die bisher nie E-Mails von Ihnen erhalten haben. bspw. Kunden, potentielle Geschäftspartner und andere. Andere Lösungen sind in diesem Fall erforderlich.

Wenn Sie einen E-Mail Client benutzen in den sich Acronis Internet Security Suite 2010 integriert, versuchen Sie folgendes:

1. Zeige Erkennungsfehler. Dadurch wird der Bayesian Filter trainiert, (Teil des Antispam Filters) und es hilft zukünftig, Erkennungsfehler zu verhindern. Der Bayesian Filter analysiert die Nachrichten und lernt ihr Muster. Die nächsten E-Mail-Nachrichten, die die gleiche Muster haben, werden nicht als `[spam]` markiert.
2. Antispam Sicherheitsstufe reduzieren. Indem die Sicherheitsstufe reduziert wird, benötigt der Antispam Filter mehr Spamanzeigen, um eine E-Mail-Nachricht als Spam einzustufen. Probieren Sie diese Lösung nur, wenn legitime Nachrichten (inklusive kommerzielle Nachrichten) fälschlicherweise als Spam erkannt werden.
3. Bayesian Filter neu trainieren. Probieren Sie diese Lösung nur, wenn vorangegangene Lösung keinen Erfolg gebracht haben.



Anmerkung

Acronis Internet Security Suite 2010 integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam Toolbar. Um die komplette Liste der unterstützen E-Mail Clients, lesen Sie bitte: *„Unterstützte Software“* (S. 2).

Wenn Sie einen anderen Mail Client benutzen, können Sie keine Erkennungsfehler angeben und den Bayesian Filter trainieren. Um das Problem zu lösen, versuchen Sie den Antispam Schutz herabzusetzen.

Kontakte zur Freundesliste hinzufügen

Wenn Sie einen unterstützten E-Mail Client verwenden, können Sie den Absernder ganz leicht zu der Freundesliste hinzufügen. Folgen Sie diesen Schritten:

1. Wählen Sie in Ihrem Mail Client eine Mail eines Senders, den Sie der Freundesliste hinzufügen möchten.
2. Klicken Sie auf **Freund hinzufügen** in der Acronis Internet Security Suite 2010 Antispam Toolbar.
3. Es kann sein das Sie die Adressen, die zur Freundesliste hinzugefügt wurden, bestätigen müssen. Wählen Sie **Diese Nachricht nicht mehr anzeigen** und klicken Sie **OK**.

Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.

Falls Sie einen anderen Mail Client verwenden, können Sie von der Acronis Internet Security Suite 2010 Oberfläche aus Kontakte der Freundesliste hinzufügen. Folgen Sie diesen Schritten:

1. Öffnen Sie Acronis Internet Security Suite 2010 und wechseln Sie in die Profi-Ansicht.
2. Klicken Sie auf **Antispam** im Menü auf der linken Seite.

3. Klicken Sie auf das **Status** Tab.
4. Klicken Sie auf **Freunde verwalten**. Ein Konfigurationsfenster wird sich öffnen.
5. Geben Sie die E-Mail Adresse ein, von der Sie E-Mail Nachrichten erhalten wollen und klicken , um die Adresse zur Freunde Liste hiunzu zu fügen.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Erfassungsfehler anzeigen

Wenn Sie einen unterstützten Mail Client verwenden, können Sie einfach den Antispam Filter korrigieren (indem Sie angeben welche E-Mail Nachrichten nicht als `[spam]`). Dadurch wird die Effektivität des Antispam Filters erheblich verbessert. Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin verschoben werden.
3. Wählen Sie die Nachricht die von Acronis Internet Security Suite 2010 fälschlicherweise als `[spam]` markiert wurde.
4. Klicken Sie auf **Freund hinzufügen** in der Acronis Internet Security Suite 2010 Antispam Toolbar. Klicken Sie zur Bestätigung **OK**. Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.
5. Klicken Sie **Kein Spam** auf der Acronis Internet Security Suite 2010 Antispam Toolbar (Normalerweise im oberen Teil des Mail Client Fensters). Dies sagt den Bayesian Filter, dass die ausgewählte Nachricht kein Spam ist. Die Nachricht wird dann in den Posteingang verschoben. Die nächsten E-Mails, die dem gleichen Muster entsprechen, werden nicht als `[spam]` markiert.

Antispam Sicherheitsstufe herabsetzen.

Um die Antispam Sichereitsstufe herabzusetzen, folgen Sie diese Schritte:

1. Öffnen Sie Acronis Internet Security Suite 2010 und wechseln Sie in die Profi-Ansicht.
2. Klicken Sie auf **Antispam** im Menü auf der linken Seite.
3. Klicken Sie auf das **Status** Tab.
4. Verschieben Sie den Schieber auf der Skala nach unten.

Es wird empfohlen den Schutz um nur eine Stufe herabzusetzen und nach einer ausreichenden Zeit die Resultate zu sichten. Wenn weiterhin legitime E-Mail Nachrichten als `[spam]` markiert werden, können sie den Schutz-Grad weiter herabstufen. Stellen Sie fest, dass viele Nachrichten nicht als Spam erkannt werden, sollten Sie den Schutz-Grad nicht herabsetzen.

Trainieren Sie den Bayesian Filter

Bevor Sie den Bayesian Filter tranieren, erstellen Sie einen Ordner der einen der legitimen Nachrichten enthält und sonst nur SPAM Nachrichten. Der Bayesian Filter wird trainiert, indem er sie analysiert und lernt die Charakteristiken, die Spam und legitime Nachrichten definieren, zu unterscheiden. Um die Effektivität des Trainings zu gewährleisten, müssen midestens 50 Nachrichten jeder Kategorie vorhanden sein.

Um die Bayesian Datenbank zurückzusetzen und um es neu zu trainieren, follgen Sie diese Schritte:

1. Öffnen Sie den Mail Client.
2. Bei der Acronis Internet Security Suite 2010 Antispamleiste klicken Sie auf **Assistent** um den Antispam Konfigurierungsassistent zu starten. Weitere Informationen werden zur Verfügung gestellt im Abschnitt *„Konfigurationsassistent“* (S. 277).
3. Klicken Sie auf **Weiter**.
4. Wählen Sie **Überspringen** und klicken Sie auf **Weiter**.
5. Wählen Sie **Antispamfilter löschen** un klicken Sie auf **Weiter**.
6. Wählen Sie den Ordner mit legitime Nachrichten und klicken Sie auf **Weiter**.
7. Wählen Sie den Ordner mit SPAM Nachrichten und klicken Sie auf **Weiter**.
8. Klichen Sie auf **Fertigstellen** um mit dem Trainingsprozess zu starten.
9. Nach Abschluss des Trainings, klicken Sie **Schließen**.

Nach Hilfe fragen

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Acronis Support wie in folgendem Abschnitt beschrieben: *„Support“* (S. 318).

33.4.2. Viele Spam Nachrichten werden nicht entdeckt.

Wenn Sie viele Nachrichten erhalten, die nicht als `[spam]` markiert sind, konfigurieren Sie den Acronis Internet Security Suite 2010 Antispam Filter, um seine Effektivität zu erhöhen.

Wenn Sie einen E-Mail Client benutzen mit dem sich Acronis Internet Security Suite 2010 integriert, versuchen Sie folgende Schritte (einzeln):

1. Indizieren Sie unentdeckte Spam Nachrichten. Dadurch wird der Bayesianische Filter trainiert (Teil des Antispam Filters) und die Antispam Erkennungsrate erhöht. Der Bayesian Filter analysiert die Nachrichten und lernt ihr Muster. Die nächsten E-Mail-Nachrichten, die die gleiche Muster haben, werden folgendermaßen markiert `[spam]`.

2. Spammer zur Spammerliste hinzufügen. Die E-Mail-Nachrichten, die von den Adressen aus der Spammerliste empfangen werden, werden automatisch markiert als [spam].
3. Antispam Sicherheitsstufe erhöhen. Indem die Sicherheitsstufe erhöht wird, benötigt der Antispam Filter weniger Spamanzeigen, um eine E-Mail-Nachricht als Spam einzustufen.
4. Trainieren Sie die lernfähige Engine (Bayesian filter) erneut. Nutzen Sie diese Lösung, wenn die Erkennungsrate des Antispam Filters sehr schlecht ist und das Anzeigen nicht markierter Nachrichten nicht funktioniert.



Anmerkung

Acronis Internet Security Suite 2010 integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam Toolbar. Um die komplette Liste der unterstützen E-Mail Clients, lesen Sie bitte: „*Unterstützte Software*“ (S. 2).

Wenn Sie einen anderen Mail Client benutzen, können Sie keine Erkennungsfehler angeben und den Bayesian Filter trainieren. Um das Problem zu lösen, versuchen Sie den Antispam Schutz heraufzusetzen und setzen Sie Spammer auf die Spammer Liste.

Zeigt unentdeckte Spam-Nachrichten

Wenn Sie einen unterstützten Mail Client verwenden, können Sie einfach angeben, welche E-Mail Nachrichten als Spam hätten markiert werden sollen. Dies wird die Effizienz des Antispam Filters erhöhen. Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Begeben Sie sich zum Inbox Ordner.
3. Wählen Sie die unentdeckte Spam-Nachricht.
4. Klicken Sie **Ist Spam** auf der Acronis Internet Security Suite 2010 Antispam Toolbar (Normalerweise im oberen Teil des Mail Client Fensters). Dies sagt den Bayesian Filter, dass die ausgewählten Nachrichten Spam sind. Sie werden dann sofort als [spam] markiert und in den Junk Mail Ordner verschoben. Die nächsten E-Mail-Nachrichten, die die gleiche Muster haben, werden folgendermaßen markiert [spam].

Spammer zu Liste der Spammer hinzufügen

Wenn Sie einen unterstützten E-Mail Client verwenden, können Sie den Absernder der Spamnachricht ganz leicht zu der Spammerliste hinzufügen. Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.

2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin verschoben werden.
3. Wählen Sie die Nachricht die von Acronis Internet Security Suite 2010 als [spam] markiert wurde.
4. Klicken Sie auf **Spammer hinzufügen** von der Acronis Internet Security Suite 2010 Antispamleiste.
5. Es kann sein das Sie die Adresse bestätigen müssen, die in der Spammerliste hinzugefügt wurde. Wählen Sie **Diese Nachricht nicht mehr anzeigen** und klicken Sie **OK**.

Benutzen Sie einen anderen Mail Client, können Sie manuell von der Acronis Internet Security Suite 2010 Benutzeoberfläche aus Spammer der Spammer Liste hinzufügen. Machen Sie dieses, wenn Sie mehrere Spam Nachrichten vom gleichen Absender erhalten haben. Folgen Sie diesen Schritten:

1. Öffnen Sie Acronis Internet Security Suite 2010 und wechseln Sie in die Profi-Ansicht.
2. Klicken Sie auf **Antispam** im Menü auf der linken Seite.
3. Klicken Sie auf das **Status** Tab.
4. Klicken Sie auf **Spammer verwalten**. Ein Konfigurationsfenster wird sich öffnen.
5. Geben Sie die E-Mail Adresse des Spammer ein und klicken , um die Adresse zur Spammer Liste hinzu zu fügen.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Erhöhen Sie die Antispam Schutzstufe

Um die Antispam Schutzstufe zu erhöhen, folgen Sie diese Schritte:

1. Öffnen Sie Acronis Internet Security Suite 2010 und wechseln Sie in die Profi-Ansicht.
2. Klicken Sie auf **Antispam** im Menü auf der linken Seite.
3. Klicken Sie auf das **Status** Tab.
4. Verschieben Sie den Schieber höher auf der Skala.

Trainieren Sie den Bayesian Filter

Bevor Sie den Bayesian Filter tranieren, erstellen Sie einen Ordner der einen der legitimen Nachrichten enthält und sonst nur SPAM Nachrichten. Der Bayesian Filter wird trainiert, indem er sie analysiert und lernt die Charakteristiken, die Spam und legitime Nachrichten definieren, zu unterscheiden. Um die Effektivität des Trainings zu gewährleisten, müssen midestens 50 Nachrichten in jedem Ordner sein.

Um die Bayesian Datenbank zurückzusetzen und um es neu zu trainieren, follgen Sie diese Schritte:

1. Öffnen Sie den Mail Client.
2. Bei der Acronis Internet Security Suite 2010 Antispamleiste klicken Sie auf **Assistent** um den Antispam Konfigurierungsassistent zu starten. Weitere Informationen werden zur Verfügung gestellt im Abschnitt *„Konfigurationsassistent“* (S. 277).
3. Klicken Sie auf **Weiter**.
4. Wählen Sie **Überspringen** und klicken Sie auf **Weiter**.
5. Wählen Sie **Antispamfilter löschen** un klicken Sie auf **Weiter**.
6. Wählen Sie den Ordner mit legitime Nachrichten und klicken Sie auf **Weiter**.
7. Wählen Sie den Ordner mit SPAM Nachrichten und klicken Sie auf **Weiter**.
8. Klichen Sie auf **Fertigstellen** um mit dem Trainingsprozess zu starten.
9. Nach Abschluss des Trainings, klicken Sie **Schließen**.

Nach Hilfe fragen

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Acronis Support wie in folgendem Abschnitt beschrieben: *„Support“* (S. 318).

33.4.3. Antispam-Filter entdeckt keine Spamnachrichten.

Wenn keine Nachrichten als `[spam]`, könnte es möglicherweise ein Problem mit dem Acronis Internet Security Suite 2010 Antispam Filter sein. Vor der Fehlersuche dieses Problems, sollten Sie sicherstellen , dass es nicht durch einen der folgenden Bedingungen verursacht wird:

- Der Acronis Internet Security Suite 2010 Antispam Schutz ist nur für die E-Mail Clients vorhanden, die konfiguriert sind, E-Mail Nachrichten über das POP3-Protokoll zu empfangen. Das bedeutet folgendes:
  - Die E-Mail-Nachrichten, die über web-basierte E-Mail-Dienstleistungen empfangen werden (wie Yahoo, Gmail, Hotmail oder andere) werden von Acronis Internet Security Suite 2010 nicht durch Spam gefiltert.
  - Wenn Ihr E-Mail Client konfiguriert ist, E-Mail Nachrichten unter Verwendung anderer Protokolle als POP3 zu empfangen (z.B., IMAP4), überprüft der Acronis Internet Security Suite 2010 Antispam Filter diese nicht auf Spam.



Anmerkung

POP3 ist eines der am meisten benutzten Protokolle für das Downloaden der E-Mail-Nachrichten vom Mail-Server. Falls Sie das Protokoll nicht kennen, das von

Ihrem E-Mail Client benutzt wird, um E-Mail Nachrichten herunterzuladen, fragen Sie die Person, die Ihren E-Mail Client konfiguriert hat.

- Acronis Internet Security Suite 2010 überprüft keine POP3-Übertragungen von Lotus Notes.

Sie sollten ausserdem die folgenden möglichen Ursachen nachprüfen:

1. Vergewissern Sie sich dass Antispam aktiviert ist.
   a. Öffnen Sie Acronis Internet Security Suite 2010.
   b. Klicken Sie oben rechts im Fenster den **Einstellungen** Schalter.
   c. Überprüfen Sie in der Kategorie Sicherheitseinstellungen den Antispamstatus.

   Falls Antispam deaktiviert ist, so liegt hier der Grund ihres Problems. Aktiviere Antispam und überwache den Antispam-Betrieb um zu erkennen ob das Problem behoben wurde.
2. Auch wenn es sehr unwahrscheinlich ist, sollten Sie überprüfen ob Acronis Internet Security Suite 2010 konfiguriert ist, SPAM-Nachrichten nicht als `[spam]` zu markieren.
   a. Öffnen Sie Acronis Internet Security Suite 2010 und wechseln Sie in die Profi-Ansicht.
   b. Klicken Sie auf **Update** im Baummenu und dann auf den Tab **Einstellungen** um diesen Bereich zu öffnen.
   c. Stellen Sie sicher das die Option **Spam-Nachrichten im Betreff markieren** ausgewählt ist.

Eine Lösung wäre es das Produkt zu reparieren oder erneut zu installieren. Falls Sie dennoch den Acronis Inc. Support kontaktieren möchten, folgen Sie der Beschreibung wie im Abschnitt *„Support“* (S. 318) beschrieben.

33.5. Entfernen von Acronis Internet Security Suite 2010 fehlgeschlagen

Dieser Artikel hilft Ihnen bei Fehlern, die auftreten können, wenn Sie Acronis Internet Security Suite 2010 deinstallieren. Es gibt zwei mögliche Situationen:

- Während der Deinstallation, erscheint ein Störungsfenster. Das Fenster bietet die Möglichkeit ein Deinstallations-Tool auszuführen, das Ihr System bereinigt.
- Die Deinstallation hängt und möglicherweise friert Ihr System ein. Klicken Sie auf **Abbrechen** um die Deinstallation abzubrechen. Wenn das nicht funktionieren sollte, starten Sie Ihren Rechner neu.

Falls die Deinstallation fehlschlägt, bleiben einige Acronis Internet Security Suite 2010 Registry-Schlüssel und Dateien in Ihrem System. Solche Rückstände können eine erneute Installation verhindern. Ebenso kann die Systemleistung und Stabilität leiden. Um den Acronis Internet Security Suite 2010 vollständig von Ihrem System zu entfernen führen Sie das "Uninstall Tool" aus.

Wenn die Deinstallation mit einer Fehlermeldung fehlschlägt, klicken Sie die Schaltfläche um das "Uninstall Tool" zu starten und das System zu bereinigen. Andernfalls gehen Sie folgendermaßen vor:

1. Kontaktieren Sie, wie unter *„Support“* (S. 318) beschrieben, den technischen Support von Acronis und fragen Sie nach dem Deinstallations-Tool.
2. Starten Sie das Uninstall Tool durch benutzung der Adminstratorrechte. Das Uninstall Tool entfernt alle Dateien und Registryeinträge welche durch die automatische Deinstallation nicht entfernt wurden.
3. Bitte starten Sie Ihren Computer neu.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Acronis Support wie in folgendem Abschnitt beschrieben: *„Support“* (S. 318).

34. Support

Wenn Sie Hilfe oder weitere Informationen zu Acronis Internet Security Suite 2010 wünschen, verwenden Sie die unten angebotenen Kontaktdaten.

Acronis Germany Gmbh
Balanstr. 59
81541 München
Deutschland

Kaufen: http://www.acronis.de/buy/purl-ais2010-de

Web: http://www.acronis.de/homecomputing/products/internet-security/

Um den Support zu kontaktieren benutzen Sie das Webformular unter http://www.acronis.de/support/ > Kontakt > Starten Sie hier.

Erreichbarkeit:

- Montag - Freitag:
  - 08:00 – 18:00 Support in Deutsch
  - 18:00 – 08:00 Support in Englisch
- Am Wochenende Support in Englisch

Medien:

- E-Mail (Webmail): in Deutsch 24x7
- Chat: abhängig von der Verfügbarkeit der Sprache
- Telefon: abhängig von der Verfügbarkeit der Sprache

Glossar

AktiveX

AktiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann.Die AktiveX Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden.Mit AktiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen.AktiveX Controls werden oft in Visual Basic geschrieben.

Erwähnenswert ist, dass bei AktiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, AktiveX über das Internet zu nutzen.

Adware

Adware ist häufig mit einer Absenderanwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware Anwendungen müssen in der Regel installiert werden, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

Archive

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einer Datensicherung/BackUp erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Verwalter absichtlich hinterlässt.Der Grund dafür muss nicht immer bösartig sein.Manche Betriebssysteme haben schon bei der Fabrikation privilegierte Konten, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Bootsektor

Der erste Sektor einer Festplatte oder Diskette.Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus

Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert.Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert.Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Durchsuchen

Kurzform für Web-Browser, eine Softwareanwendung, die zum Lokalisieren und Anzeigen von Webseiten verwendet wird.Die bekanntesten Browser sind Netscape Navigator und Microsoft Internet Explorer.Beide sind graphische Browser, das heißt sie können sowohl Grafiken als auch Texte anzeigen.Weiterhin können die meisten Browser Multimedia-Informationen wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Cookie

In der Internetindustrie werden Cookies als kleine Dateien beschrieben, die Daten über einzelne Computer enthalten und die von den Werbern analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden.Die Cookie-Technologie wurde deshalb weiter entwickelt, damit der Benutzer nur solche Werbung zugeschickt bekommt, die seinen Interessen dient.Für viele ist es aber wie ein zweischneidiges Messer.Einerseits ist es wirksam und sachbezogen, da man nur Anzeigen, an denen man interessiert ist, betrachten kann, anderseits heißt es dem Benutzer "auf die Spur zu kommen" und ihn auf Schritt und "Klick " zu verfolgen.Es ist verständlich, dass der Datenschutz ein umstrittenes Thema ist und viele sich von dem Begriff als SKU-Nummern (die Streifencodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden, angegriffen fühlen.Auch wenn dieser Gesichtspunkt extrem erscheint ist er manchmal korrekt.

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

Download

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät.Der Begriff bezeichnet oft den Kopiervorgang von einem Online Service auf den eigenen Rechner.Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.

E-Mail

Elektronische Post. Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.

Ereignisanzeige

Ereignisse oder Erscheinungen, die in einem Programm vorkommen.Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Fehlalarm

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist. Kann bei heuristischem Virenprüfen auftreten.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS.Sie enthalten gewöhnlich ein bis zwei Buchstaben (alte Betriebssysteme können nicht mehr als drei Buchstaben unterstützen), Beispiele dafür sind "c" für C-Quellcode, "ps" für PostScript oder "txt" für beliebige Texte.Windows zeigt bei ihm bekannten Dateitypen keine Dateierweiterung in der graphischen Benutzeroberfläche an, stattdessen wird häufig ein Symbol verwendet.

Heuristik

Eine Methode, um neue Viren zu identifizieren.Diese Prüfmethode beruht nicht auf spezifische Virussignaturen.Der Vorteil einer heuristischen Prüfung ist, dass man nicht von einer neuen Virusvariante getäuscht werden kann.Manchmal kann auch ein verdächtiger Code in einemnormalen Programm gemeldet werden, ein sogenannter Fehlalarm wird angezeigt.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Java Applet

Ein Java Programm, das nur auf Webseiten läuft.Um ein Applet auf einer Webseite zu benutzen, gibt man den Namen und die Größe (Länge und Breite in Pixel) des Applets an.Wenn die Webseite abgerufen wird, lädt der Browser

das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus.Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden.

Obwohl Applets auf dem Client laufen, können diese keine Daten auf der Clientmaschine lesen oder schreiben.Zusätzlich sind die Applets weiter begrenzt, so dass sie nur Daten aus der Domäne lesen und beschreiben können, die sie unterstützen.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird.Viele Anwendungen, wie Microsoft Word und Excel, unterstützen mächtige Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

E-Mail Client

Ein E-Mail Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.

Arbeitsspeicher

Interne Speicherzonen im Rechner.Der Begriff Arbeitsspeicher bedeutet Datenträger in Form von sehr schnellen Chips.Das Wort Speicher ist der Speicherplatz, der sich auf Magnetbändern oder Datenträgern befindet.Jeder Rechner hat eine gewisse Menge Arbeitsspeicher.Dieser wird auch Hauptspeicher oder RAM genannt.

Nicht heuristisch

Diese Prüfmethode beruht auf einer spezifischen Virussignatur.Der Vorteil einer nicht heuristischen Prüfung ist, dass diese nicht von einem Scheinvirus getäuscht werden kann, und dass dieser keinen falschen Alarm auslöst.

Komprimierte Programme

Eine Datei in einem komprimierten Format.Viele Betriebssysteme und Anwendungen enthalten Befehle, die das Komprimieren einer Datei ermöglichen, so dass diese weniger Speicherplatz benötigt.Zum Beispiel: Angenommen Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält.Normalerweise nehmen diese 10 Bytes Speicherplatz ein.

Ein Programm, das Dateien komprimiert, würde die Leerzeichen durch ein spezielles Zeichen „Leerzeichenreihe“ ersetzen, gefolgt von der Zahl der Leerzeichen, die ersetzt wurden.In diesem Fall sind nur noch zwei Bytes notwendig statt zehn.Das wäre ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.

Pfad

Zeigt die Stelle an, an der sich eine Datei in einem Rechner befindet.Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses: Laufwerke, Ordner, Unterverzeichnisse, die Datei und ihre Erweiterung.

Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.

Phishing

Dabei wird eine E-Mail mit einer betrügerischen Absicht an einen Nutzer gesendet.Der Inhalt dieser E-Mail gibt vor, von einem bekannten und seriös arbeitenden Unternehmen zu stammen.Zweck dieser E-Mail ist es dann, private und geheime Nutzerdaten zu erhalten, worauf der Absender beabsichtigt, die Identität des Nutzers anzunehmen.Die E-Mail führt den Benutzer dann auf eine Webseite, in der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TAN's oder PIN's preiszugeben.Dies soll aus Gründen der Aktualisierung geschehen.Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert.Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann.Rechner haben verschiedenartige Schnittstellen.Intern gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen.Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen.Die Schnittstellennummer gibt die Art der Schnittstelle an.Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert Acronis Internet Security Suite 2010 eine Logdatei mit die geprüften Pfaden, Ordnern und der Archivanzahl, aber auch die geprüften, infizierten oder verdächtigen Dateien.

Rootkit

Bei einem Rootkit handelt es sich um einen Satz von Softwarewerkzeugen die einem Administrator Low-End Zugriff zu einem System verschaffen. Rootkits traten zunächst nur auf UNIX-Systemen auf und haben im Laufe der Zeit auch Ihren Einzug auf Linux- und Windows-Systemen gehalten.

Die Hauptaufgabe eines Rootkits besteht darin, seine Existenz zu verstecken indem Prozesse und Dateien versteckt werden, Anmeldedaten und Berichtsdateien zu fälschen und jegliche Art von Daten abzufangen.

Rootkits zählen von Haus aus nicht zu schadensverursachender Software da Sie keine Schadroutinen besitzen. Jedoch verändern Sie die vom Betriebssystem zurückgegebenen Daten und verstecken auf diese Weise ihre Präsenz. Dennoch kann über ein solches Rootkit schädliche Software nachträglich eingeschleust werden und auch der wirtschaftliche Schaden ist nicht zu unterschätzen.

Script

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer Anwenderdaten über seine Internetverbindung sammelt und abruft. Dies geschieht in der Regel zu Werbezwecken. Typischerweise werden Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Sharewareprogrammen gebündelt, die aus dem Internet herunter geladen werden können. Es ist jedoch darauf hinzuweisen, dass die Mehrzahl der Shareware- und Freeware-Anwendungen frei von Spyware ist. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an jemand anderen. Spyware kann auch Informationen über E-Mail Adressen und sogar Kennwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren.Eine weit verbreitete Möglichkeit, ein Opfer von Spyware zu werden, ist der Download von bestimmten heute erhältlichen Peer-to-Peer-Dateiaustauschprogrammen (Direktverbindungen von Computern).

Abgesehen von den Fragen der Ethik und des Datenschutzes bestiehlt Spyware den Anwender, indem sie Speicherressourcen seines Rechners nutzt und den Internetzugriff verlangsamt, indem über seine Internetverbindung Informationen an den Spyware-Heimatserver gesendet werden.Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Startup Objekt (Autostart-Objekt)

Jede Datei, die sich in diesem Ordner befindet, öffnet sich, wenn der Rechner gestartet wird.Zum Beispiel ein Startbildschirm, eine Sounddatei, die abgespielt wird, wenn der Rechner gestartet wird, ein Erinnerungskalender oder

Anwendungsprogramme können Autostart-Objekte sein.Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.

Symbolleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Taskleiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet).Er enthält kleine Icons zur Information und zum leichteren Zugriff, zum Beispiel: Fax, Drucker, Modem, Lautstärke und mehr.Um auf die Details und Steuerungen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol - Im Internet werden eine Vielzahl von verschiedener Hardware und Betriebssystemen miteinander verbunden.TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein vernichtendes Programm, das sich als eine freundliche Anwendung tarnt und auftritt.Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können zerstörerisch sein.Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert.Viele Trojaner öffnen den Rechner für den Zugriff von außen.

Der Begriff entstammt einer Geschichte in Homer's "Ilias", in der die Griechen Ihren Feinden, den Trojanern, angeblich als Sühnegabe ein hölzernes Pferd schenkten.Aber, nachdem die Trojaner das Pferd innerhalb der Stadtmauern gebracht hatten, kamen die in dem Bauch des hölzernen Pferdes versteckten Soldaten heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsmännern in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Aktualisierung

Neue Softwareversionen oder Hardwareprodukte, die eine ältere Version ersetzen.Die Update-Installationsroutine sucht nach älteren Versionen auf dem Rechner, da sonst kein Update installiert werden kann.

Acronis Internet Security Suite 2010 hat sein eigenes Update Modul, welches das manuelle oder automatische Prüfen nach Updates ermöglicht.

Virus

Ein Programm oder ein Codestück, das auf einen Rechner geladen wird, ohne dass der Benutzer Kenntnis davon hat und welches sich allein ausführt.Die Resultate von Viren können einfache Scherzmeldungen aber auch die Zerstörung von Hardware sein.Die meisten Viren können sich selber vervielfältigen.Alle Computerviren sind von Menschenhand geschrieben.Ein Virus, der sich immer wieder vervielfältigen kann ist sehr einfach zu schreiben.Sogar ein solch

einfacher Virus ist fähig, sich durch Netzwerke zu verschicken und Sicherheitssysteme zu überbrücken.

Virusdefinition

Ein binäres Virusmuster, das von einem AntiVirus Programm verwendet wird, um einen Virus zu entdecken und zu entfernen.

Wurm

Ein Programm, das sich über ein Netzwerk verbreitet.Es kann sich nicht an andere Programme anhängen.